Developer Guide

# AWS Config

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Config: Developer Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

# Table of Contents

**What Is AWS Config? ... 1**
Considerations ... 1
Ways to Use AWS Config ... 1
Resource Administration ... 1
Auditing and Compliance ... 2
Managing and Troubleshooting Configuration Changes ... 2
Security Analysis ... 2
Partner Solutions ... 3
Features ... 3
How AWS Config Works ... 4
Resource Discovery ... 5
Resource Tracking ... 5
Delivery of Configuration Items ... 6
Control Access to AWS Config ... 9
Terminology and concepts ... 9
AWS Config Interfaces ... 10
Resource Management ... 11
Configuration Recorder ... 12
Delivery Channel ... 6
AWS Config Rules ... 14
Conformance Packs ... 17
Aggregators ... 18
AWS Service Integrations ... 19
AWS Organizations ... 19
AWS Control Tower ... 19
AWS CloudTrail ... 19
AWS Security Hub CSPM ... 20
AWS Trusted Advisor ... 20
AWS Audit Manager ... 21
AWS Systems Manager ... 21
AWS Firewall Manager ... 21
Amazon EC2 Dedicated Hosts ... 22
Application Load Balancers ... 22
AWS CodeBuild ... 22

AWS X-Ray ... 23
AWS Service Management Connector ... 23
Amazon API Gateway ... 23
Region Support ... 23
Considerations ... 23
List of Supported Regions ... 24
Service Limits ... 29
Supplemental Information ... 31
AWS Software Development Kits for AWS Config ... 32
**Getting Started ... 34**
Signing up for AWS ... 34
Sign up for an AWS account ... 34
Create a user with administrative access ... 35
Ways to Get Started with AWS Config ... 36
Setting Up (Console) ... 36
Setting up ... 36
1-click setup ... 37
Manual setup ... 40
Setting Up (AWS CLI) ... 47
Setting up ... 47
Prerequisites ... 48
Starting AWS Config ... 114
Verifying setup ... 117
Working with AWS SDKs ... 119
**Configuration Recorder ... 121**
Considerations for the customer managed configuration recorder ... 122
Considerations for service-linked configuration recorders ... 123
Supported services ... 124
Drift detection for the configuration recorder ... 125
Starting the customer managed configuration recorder ... 126
Stopping the customer managed configuration recorder ... 126
Changing the recording frequency for the customer managed configuration recorder ... 127
Renaming the customer managed configuration recorder ... 130
Viewing your configuration recorders ... 131
Deleting your configuration recorders ... 132
**Delivery Channel ... 134**

Considerations ... 134
Terminology ... 135
Components of a Configuration Item ... 136
Viewing the Delivery Channel ... 138
Updating the Delivery Channel ... 139
Renaming the Delivery Channel ... 144
Delivering Configuration Snapshots ... 145
Delivering Configuration Snapshots ... 146
Verifying Delivery Status ... 146
Viewing Configuration Snapshots ... 147
Viewing Configuration Snapshots ... 147
Example Configuration Snapshot ... 148
Example Notifications ... 153
Example Configuration Item Change Notifications ... 154
Example Configuration History Delivery Notification ... 167
Example Configuration Snapshot Delivery Started Notification ... 168
Example Configuration Snapshot Delivery Notification ... 169
Example Compliance Change Notification ... 170
Example Rules Evaluation Started Notification ... 173
Example Oversized Configuration Item Change Notification ... 174
Example Delivery Failed Notification ... 177
**AWS Config Dashboard ... 179**
Compliance and Resource Inventory ... 179
AWS Config Usage and Success Metrics ... 181
**Resource Management ... 184**
Supported Resource Types ... 185
Amazon AppStream ... 186
Amazon AppFlow ... 186
... 187
Amazon API Gateway ... 187
Amazon Athena ... 188
Amazon Bedrock ... 188
Amazon Bedrock AgentCore ... 189
Amazon CloudFront ... 189
Amazon CloudWatch ... 190
Amazon CodeGuru ... 191

Amazon Cognito ..... 191
Amazon Comprehend ..... 192
Amazon Connect ..... 192
Amazon Detective ..... 193
Amazon DynamoDB ..... 194
Amazon EC2 ..... 194
Amazon ECR ..... 204
Amazon ECS ..... 204
Amazon EFS ..... 205
Amazon EKS ..... 206
Amazon EMR ..... 206
Amazon EMR Serverless ..... 207
Amazon EventBridge ..... 207
Amazon Forecast ..... 208
Amazon Fraud Detector ..... 208
Amazon GameLift ..... 209
Amazon GuardDuty ..... 209
Amazon Inspector ..... 210
Amazon IVS ..... 210
Amazon Keyspaces ..... 211
Amazon Location Service ..... 211
Amazon OpenSearch Service ..... 211
Amazon Personalize ..... 213
Amazon Pinpoint ..... 213
Amazon QLDB ..... 214
Amazon Kendra ..... 214
Amazon Kinesis ..... 215
Amazon Lex ..... 215
Amazon Lightsail ..... 216
Amazon Lookout for Metrics ..... 216
Amazon Lookout for Vision ..... 217
Amazon Macie ..... 217
Amazon Managed Grafana ..... 217
Amazon Managed Service for Prometheus ..... 217
Amazon MemoryDB ..... 218
Amazon MQ ..... 218

Amazon MSK ..... 218
Amazon Quick Suite ..... 219
Amazon Redshift ..... 219
Amazon RDS ..... 221
Amazon Route 53 ..... 222
Amazon SageMaker AI ..... 224
Amazon SES ..... 226
Amazon SNS ..... 227
Amazon SQS ..... 227
Amazon S3 ..... 228
Amazon WorkSpaces ..... 230
AWS Amplify ..... 231
AWS AppConfig ..... 231
AWS App Runner ..... 232
AWS App Mesh ..... 232
AWS AppSync ..... 233
AWS Audit Manager ..... 233
AWS Auto Scaling ..... 234
AWS B2B Data Interchange ..... 234
AWS Backup ..... 235
AWS Batch ..... 236
AWS Billing and Cost Management ..... 236
AWS Budgets ..... 236
AWS Certificate Manager ..... 237
AWS Clean Rooms ..... 237
AWS CloudFormation ..... 237
AWS CloudTrail ..... 238
AWS Cloud9 ..... 238
AWS Cloud Map ..... 239
AWS CodeArtifact ..... 239
AWS CodeBuild ..... 240
AWS CodeDeploy ..... 240
AWS CodePipeline ..... 241
AWS Config ..... 241
AWS DMS ..... 243
AWS DataSync ..... 243

AWS Deadline Cloud ..... 245
AWS Device Farm ..... 245
AWS Elastic Beanstalk ..... 246
AWS Entity Resolution ..... 246
AWS FIS ..... 247
AWS Global Accelerator ..... 247
AWS Glue ..... 248
AWS Ground Station ..... 248
AWS HealthLake ..... 249
AWS IAM ..... 249
AWS IoT ..... 251
AWS KMS ..... 255
AWS Lambda ..... 255
AWS Mainframe Modernization ..... 255
AWS Network Firewall ..... 256
AWS Network Manager ..... 256
AWS Organizations ..... 258
AWS Panorama ..... 258
AWS Private CA ..... 258
AWS Resilience Hub ..... 259
AWS Resource Explorer ..... 260
AWS RoboMaker ..... 260
AWS Signer ..... 260
AWS Secrets Manager ..... 261
AWS Security Hub CSPM ..... 261
AWS Service Catalog ..... 261
AWS Shield ..... 262
AWS Step Functions ..... 263
AWS Systems Manager ..... 263
AWS Transfer Family ..... 264
AWS WAF ..... 265
AWS X-Ray ..... 267
Elastic Load Balancing ..... 267
MediaConnect ..... 268
MediaPackage ..... 269
MediaTailor ..... 270

Resource Coverage by Region Availability ..... 270
North and South America ..... 270
Europe ..... 322
Asia Pacific ..... 365
China ..... 422
Africa and Middle East ..... 447
GovCloud ..... 481
Recording AWS Resources ..... 508
Considerations ..... 509
Regional and global Resources ..... 510
AWS Config Rules and global resource types ..... 513
Recording frequency ..... 514
Non-recorded resources ..... 515
Recording resources (Console) ..... 516
Recording resources (AWS CLI) ..... 520
Excluding resources ..... 527
Stopping recording ..... 528
Recording Third-Party Resources (AWS CLI) ..... 528
Adding Resources ..... 529
Recording Configuration Items ..... 533
Reading Configuration Items ..... 534
Deleting Resources ..... 535
Recording Software Configurations ..... 535
Prerequisites ..... 536
Recording Software Configurations ..... 536
Looking up Resources ..... 538
Viewing Resources ..... 540
Viewing compliance (Console) ..... 540
Viewing compliance (AWS SDKs) ..... 541
Viewing Compliance History ..... 548
Viewing Compliance History (Console) ..... 549
Viewing Compliance History (AWS CLI) ..... 549
For Resources and Rules ..... 555
Querying Compliance History ..... 556
Tagging Your Resources ..... 557
Restrictions Related to Tagging ..... 558

Managing Tags with AWS Config API Actions ... 558
**AWS Config Rules ... 560**
Considerations ... 560
Region Support ... 563
Components of a Rule ... 572
How AWS Config Rules Work ... 572
Trigger Types ... 573
Evaluation Modes ... 574
Rule Metadata ... 575
Managed Rules ... 576
List of Managed Rules ... 577
List of Managed Rules by Evaluation Mode ... 1117
List of Managed Rules by Trigger Type ... 1142
List of Managed Rules by Region Availability ... 1167
Creating Managed Rules With AWS CloudFormation Templates ... 1781
Custom Rules ... 1783
Custom Policy Rules ... 1783
Custom Lambda Rules ... 1783
Format differences for AWS Config Custom Rules ... 1784
Creating Custom Policy Rules ... 1784
Creating Custom Lambda Rules ... 1791
Managing Deleted Resources for Custom Lambda Rules ... 1813
Service-Linked Rules ... 1815
Organizational Rules ... 1816
Considerations ... 1816
Deployment ... 1817
Region Support ... 1818
Adding Rules ... 1822
Using the console ... 1822
Using the AWS SDKs ... 1825
Updating Rules ... 1829
Using the console ... 1829
Using the AWS SDKs ... 1829
Deleting Rules ... 1833
Considerations ... 1833
Using the console ... 1834

Using the AWS SDKs ... 1835
Viewing Rules ... 1836
Using the console ... 1836
Using the AWS SDKs ... 1837
Turning on Proactive Evaluation ... 1849
Using the console ... 1849
Using the AWS SDKs ... 1852
Sending Evaluations to Security Hub CSPM ... 1856
Send Rule Evaluations to Security Hub CSPM ... 1856
Evaluating Resources with Rules ... 1856
Deleting Evaluation Results ... 1861
Troubleshooting ... 1862
**Conformance Packs ... 1864**
Conformance Pack Dashboard ... 1865
Navigating the Conformance Packs Main Page ... 1865
Prerequisites ... 1866
Step 1: Start AWS Config Recording ... 1866
Step 2: Additional Prerequisites by Conformance Pack Type ... 1866
Region Support ... 1872
Process Checks ... 1880
Sample Template ... 1881
Creating Process Checks ... 1881
Changing Compliance Status ... 1882
View and Edit ... 1883
Conformance Pack Sample Templates ... 1884
AWS Control Tower Detective Guardrails Conformance Pack ... 1888
Cyber Resilience Best Practices for Amazon S3, Amazon EBS, and Amazon DynamoDB ... 1888
Operational Best Practices for ABS CCIG 2.0 Material Workloads ... 1889
Operational Best Practices for ABS CCIG 2.0 Standard Workloads ... 2098
Operational Best Practices for ACSC Essential 8 ... 2248
Operational Best Practices for ACSC ISM - Part 1 ... 2272
Operational Best Practices for ACSC ISM - Part 2 ... 2400
Operational Best Practices for AI and ML ... 2409
Operational Best Practices for Amazon API Gateway ... 2409
Operational Best Practices for Amazon CloudWatch ... 2409
Operational Best Practices for Amazon DynamoDB ... 2409

Operational Best Practices for Amazon S3 ..... 2409
Operational Best Practices for APRA CPG 234 ..... 2410
Operational Best Practices for Asset Management ..... 2623
Operational Best Practices for AWS Backup ..... 2624
Operational Best Practices for AWS Identity And Access Management ..... 2624
Operational Best Practices for AWS Well-Architected Framework Reliability Pillar ..... 2624
Operational Best Practices for AWS Well-Architected Framework Security Pillar ..... 2688
Operational Best Practices for BCP and DR ..... 2837
Operational Best Practices for BNM RMiT ..... 2837
Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile ..... 3146
Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1 ..... 4613
Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2 ..... 4656
Operational Best Practices for CIS Critical Security Controls v8 IG1 ..... 4713
Operational Best Practices for CIS Critical Security Controls v8 IG2 ..... 4804
Operational Best Practices for CIS Critical Security Controls v8 IG3 ..... 4963
Operational Best Practices for CIS Top 20 ..... 5136
Operational Best Practices for CISA Cyber Essentials ..... 5210
Operational Best Practices for Criminal Justice Information Services (CJIS) ..... 5397
Operational Best Practices for CMMC 2.0 Level 1 ..... 5521
Operational Best Practices for CMMC 2.0 Level 2 ..... 5635
Operational Best Practices for Compute Services ..... 6016
Operational Best Practices for Data Resiliency ..... 6017
Operational Best Practices for Databases Services ..... 6017
Operational Best Practices for Data Lakes and Analytics Services ..... 6017
Operational Best Practices for DevOps ..... 6017
Operational Best Practices for EC2 ..... 6018
Operational Best Practices for Encryption and Key Management ..... 6018
Operational Best Practices for ENISA Cybersecurity guide for SMEs ..... 6018
Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low ..... 6174
Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium ..... 6279
Operational Best Practices for Esquema Nacional de Seguridad (ENS) High ..... 6394
Operational Best Practices for FDA Title 21 CFR Part 11 ..... 6518
Operational Best Practices for FedRAMP(Low) ..... 6842
Operational Best Practices for FedRAMP(Moderate) ..... 7094
Operational Best Practices for FedRAMP (High Part 1) ..... 7627

Operational Best Practices for FedRAMP (High Part 2) ..... 8212
Operational Best Practices for FFIEC ..... 8337
Operational Best Practices for Germany Cloud Computing Compliance Criteria Catalog (C5) ..... 8550
Operational Best Practices for Gramm Leach Bliley Act (GLBA) ..... 8629
Operational Best Practices for GxP EU Annex 11 ..... 8686
Operational Best Practices for HIPAA Security ..... 8845
Operational Best Practices for IRS 1075 ..... 9323
Operational Best Practices for K-ISMS ..... 9534
Operational Best Practices for Load Balancing ..... 9617
Operational Best Practices for Logging ..... 9618
Operational Best Practices for Management and Governance Services ..... 9618
Operational Best Practices for MAS Notice 655 ..... 9618
Operational Best Practices for MAS TRMG ..... 9658
Operational Best Practices for Monitoring ..... 9866
Operational Best Practices for NBC TRMG ..... 9867
Operational Best Practices for NERC CIP BCSI ..... 10321
Operational Best Practices for NCSC Cloud Security Principles ..... 10393
Operational Best Practices for NCSC Cyber Assesment Framework ..... 10494
Operational Best Practices for Networking and Content Delivery Services ..... 10668
Operational Best Practices for NIST 800-53 rev 4 ..... 10668
Operational Best Practices for NIST 800-53 rev 5 ..... 10988
Operational Best Practices for NIST 800 171 ..... 11595
Operational Best Practices for NIST 800 172 ..... 11923
Operational Best Practices for NIST 800 181 ..... 11994
Operational Best Practices for NIST 1800 25 ..... 12470
Operational Best Practices for NIST CSF ..... 12628
Operational Best Practices for NIST Privacy Framework v1.0 ..... 12972
Operational Best Practices for NYDFS 23 ..... 13209
Operational Best Practices for NZISM 3.8 ..... 13384
Operational Best Practices for PCI DSS 3.2.1 ..... 13521
Operational Best Practices for PCI DSS 4.0 (Excluding global resource types) ..... 13845
Operational Best Practices for PCI DSS 4.0 (Including global resource types) ..... 14114
Operational Best Practices for Publicly Accessible Resources ..... 14451
Operational Best Practices for RBI Cyber Security Framework for UCBs ..... 14451
Operational Best Practices for RBI MD-ITF ..... 14497

Operational Best Practices for Security, Identity, and Compliance Services ..... 14643
Operational Best Practices for Serverless ..... 14643
Operational Best Practices for Storage Services ..... 14643
Operational Best Practices for SWIFT CSP ..... 14643
Security Best Practices for Amazon Elastic Container Service (Amazon ECS) ..... 14678
Security Best Practices for Amazon Elastic File System (Amazon EFS) ..... 14678
Security Best Practices for Amazon Elastic Kubernetes Service (Amazon EKS) ..... 14679
Security Best Practices for Amazon CloudFront ..... 14679
Security Best Practices for Amazon OpenSearch Service ..... 14679
Security Best Practices for Amazon Redshift ..... 14679
Security Best Practices for Amazon Relational Database Service (Amazon RDS) ..... 14680
Security Best Practices for AWS Auto Scaling ..... 14680
Security Best Practices for AWS CloudTrail ..... 14680
Security Best Practices for AWS CodeBuild ..... 14680
Security Best Practices for Amazon ECR ..... 14681
Security Best Practices for AWS Lambda ..... 14681
Security Best Practices for AWS Network Firewall ..... 14681
Security Best Practices for Amazon SageMaker AI ..... 14681
Security Best Practices for AWS Secrets Manager ..... 14682
Security Best Practices for AWS WAF ..... 14682
Example Templates with Remediation Action ..... 14682
Creating Custom Templates ..... 14683
Terminology ..... 14683
Customizing the template ..... 14683
Deploying Conformance Packs ..... 14688
Editing Conformance Packs ..... 14691
Deleting Conformance Packs ..... 14692
Considerations ..... 14692
To delete a conformance pack ..... 14693
Viewing Conformance Packs ..... 14694
Viewing Compliance History ..... 14697
Viewing the Compliance Timeline ..... 14697
Querying Compliance History ..... 14698
Managing Organizational Conformance Packs ..... 14700
Considerations ..... 14700
Deployment ..... 14701

Region Support ... 14702
Troubleshooting ... 14706
Failed status for a conformance pack ... 14706
Dangling rules in a conformance pack ... 14708
**Remediation ... 14710**
Region Support ... 14710
Setting Up Manual Remediation ... 14714
Setting Up Auto Remediation ... 14715
Deleting Remediation Actions ... 14718
**Aggregators ... 14719**
Use Cases ... 14719
Terminology ... 14720
Region Support ... 14720
Aggregator Dashboard ... 14725
Using the Aggregator Dashboard ... 14725
Compliance Dashboard ... 14728
Inventory Dashboard ... 14730
Creating Aggregators ... 14732
Registering a Delegated Administrator ... 14738
Editing Aggregators ... 14740
Deleting Aggregators ... 14742
Authorizing Aggregator Accounts ... 14742
Considerations ... 14743
Adding Authorization ... 14743
Deleting Authorizations ... 14745
Considerations ... 14745
Deleting Authorization ... 14745
Viewing Aggregators ... 14746
Troubleshooting ... 14747
**Advanced Queries ... 14750**
Features ... 14751
Query Components ... 14751
Synopsis ... 14751
Parameters ... 14752
Examples ... 14752
Query Editor (Console) ... 14753

Considerations ..... 14753
Use an AWS Sample Query ..... 14753
Create your custom query ..... 14754
Query Editor (AWS CLI) ..... 14755
Considerations ..... 14755
Query Resource Configuration Data ..... 14756
Save a Query ..... 14757
View all the Saved Queries ..... 14758
Get Details of a Saved Query ..... 14759
Delete a Saved Query ..... 14759
Natural language query processor ..... 14760
Considerations ..... 14760
Query using the natural language query processor ..... 14753
Example prompts ..... 14761
Providing feedback ..... 14765
Region Support ..... 14765
Examples Queries ..... 14766
Example Relationship Queries ..... 14772
Limitations ..... 14773
CIDR notation/IP range ..... 14775
Multiple properties within an array ..... 14776
Region Support ..... 14777
**Deleting Data ..... 14782**
Setting Data Retention Period (Console) ..... 14784
**Security ..... 14786**
Data Protection ..... 14787
Encryption of Data in Transit ..... 14788
Encryption of Data in Transit ..... 14788
Identity and Access Management ..... 14788
Audience ..... 14789
Authenticating with identities ..... 14789
Managing access using policies ..... 14790
How AWS Config works with IAM ..... 14792
Identity-based policy examples ..... 14797
AWS managed policies ..... 14816
Permissions for the IAM Role ..... 14996

Updating the IAM Role ... 15001
Permissions for the Amazon S3 Bucket ... 15003
Permissions for the KMS Key ... 15007
Permissions for the Amazon SNS Topic ... 15010
Troubleshooting ... 15014
Using Service-Linked Roles ... 15016
Incident Response ... 15018
Compliance Validation ... 15018
Resilience ... 15019
Infrastructure Security ... 15019
Configuration and Vulnerability Analysis ... 15019
Cross-service confused deputy prevention ... 15019
Best Practices ... 15020
**Logging and Monitoring ... 15021**
Logging ... 15021
AWS Config Information in CloudTrail ... 15021
Understanding AWS Config Log File Entries ... 15022
Example Log Files ... 15022
Monitoring ... 15030
Using Amazon SQS ... 15031
Using Amazon EventBridge ... 15033
**Amazon VPC endpoints ... 15040**
Create a VPC Endpoint ... 15040
**FAQs ... 15041**
Unable to see my latest configuration changes ... 15041
Can I expect to view my configuration changes right away? ... 15041
Indirect Relationships in AWS Config ... 15041
What is resource relationship? ... 15041
What is a direct and an indirect relationship with respect to a resource? ... 15042
Which indirect relationships does AWS Config support? ... 15042
Which scenarios uses indirect relationship? ... 15044
How are the configuration items created due to direct and indirect relationship? ... 15046
What are the configuration items generated due to indirect relationships? ... 15046
How do I disable indirect relationship? ... 15048
How do I retrieve configuration data related to indirect relationships? ... 15049
**Code examples ... 15050**

Basics ..... 15050
Actions ..... 15051
**Document History ..... 15087**
Earlier Updates ..... 15240

# What Is AWS Config?

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

An AWS *resource* is an entity you can work with in AWS, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC). For a complete list of AWS resources supported by AWS Config, see Supported Resource Types for AWS Config.

## Considerations

- **AWS account**: You need an active AWS account. For more information, see Signing up for AWS.
- **Amazon S3 Bucket**: You need an S3 bucket to receive data for your configuration snapshots and history. For more information, see Permissions for the Amazon S3 Bucket.
- **Amazon SNS Topic**: You need an Amazon SNS to receive notifications when there are changes to your configuration snapshots and history. For more information, see Permissions for the Amazon SNS Topic.
- **IAM Role**: You need an IAM role that has the necessary permissions to access AWS Config. For more information, see Permissions for the IAM Role.
- **Resource types**: You can decide which resource types you want AWS Config to record. For more information, see Recording AWS Resources.

## Ways to Use AWS Config

When you run your applications on AWS, you usually use AWS resources, which you must create and manage collectively. As the demand for your application keeps growing, so does your need to keep track of your AWS resources. AWS Config is designed to help you oversee your application resources in the following scenarios:

### Resource Administration

To exercise better governance over your resource configurations and to detect resource misconfigurations, you need fine-grained visibility into what resources exist and how these

resources are configured at any time. You can use AWS Config to notify you whenever resources are created, modified, or deleted without having to monitor these changes by polling the calls made to each resource.

You can use AWS Config rules to evaluate the configuration settings of your AWS resources. When AWS Config detects that a resource violates the conditions in one of your rules, AWS Config flags the resource as noncompliant and sends a notification. AWS Config continuously evaluates your resources as they are created, changed, or deleted.

## Auditing and Compliance

You might be working with data that requires frequent audits to ensure compliance with internal policies and best practices. To demonstrate compliance, you need access to the historical configurations of your resources. This information is provided by AWS Config.

## Managing and Troubleshooting Configuration Changes

When you use multiple AWS resources that depend on one another, a change in the configuration of one resource might have unintended consequences on related resources. With AWS Config, you can view how the resource you intend to modify is related to other resources and assess the impact of your change.

You can also use the historical configurations of your resources provided by AWS Config to troubleshoot issues and to access the last known good configuration of a problem resource.

## Security Analysis

To analyze potential security weaknesses, you need detailed historical information about your AWS resource configurations, such as the AWS Identity and Access Management (IAM) permissions that are granted to your users, or the Amazon EC2 security group rules that control access to your resources.

You can use AWS Config to view the IAM policy that was assigned to a user, group, or role at any time in which AWS Config was recording. This information can help you determine the permissions that belonged to a user at a specific time: for example, you can view whether the user `John Doe` had permission to modify Amazon VPC settings on Jan 1, 2015.

You can also use AWS Config to view the configuration of your EC2 security groups, including the port rules that were open at a specific time. This information can help you determine whether a security group blocked incoming TCP traffic to a specific port.

## Partner Solutions

AWS partners with third-party specialists in logging and analysis to provide solutions that use AWS Config output. For more information, visit the AWS Config detail page at AWS Config.

# Features

When you set up AWS Config, you can complete the following:

### Resource management

- Specify the resource types you want AWS Config to record.

- Set up an Amazon S3 bucket to receive a configuration snapshot on request and configuration history.
- Set up Amazon SNS to send configuration stream notifications.
- Grant AWS Config the permissions it needs to access the Amazon S3 bucket and the Amazon SNS topic.

  For more information, see Viewing AWS Resource Configurations and History and Managing AWS Resource Configurations and History.

### Rules and conformance packs

- Specify the rules that you want AWS Config to use to evaluate compliance information for the recorded resource types.
- Use conformance packs, or a collection of rules that can be deployed and monitored as a single entity in your AWS account.

  For more information, see Evaluating Resources with AWS Config Rules and Conformance Packs.

### Remediation

- Remediate noncompliant resources that are evaluated by AWS Config Rules.

  For more information, see Remediation.

### Aggregators

- Use an aggregator to get a centralized view of your resource inventory and compliance. An aggregator collects AWS Config configuration and compliance data from multiple AWS accounts and AWS Regions into a single account and Region.

  For more information, see Multi-Account Multi-Region Data Aggregation.

### Advanced queries

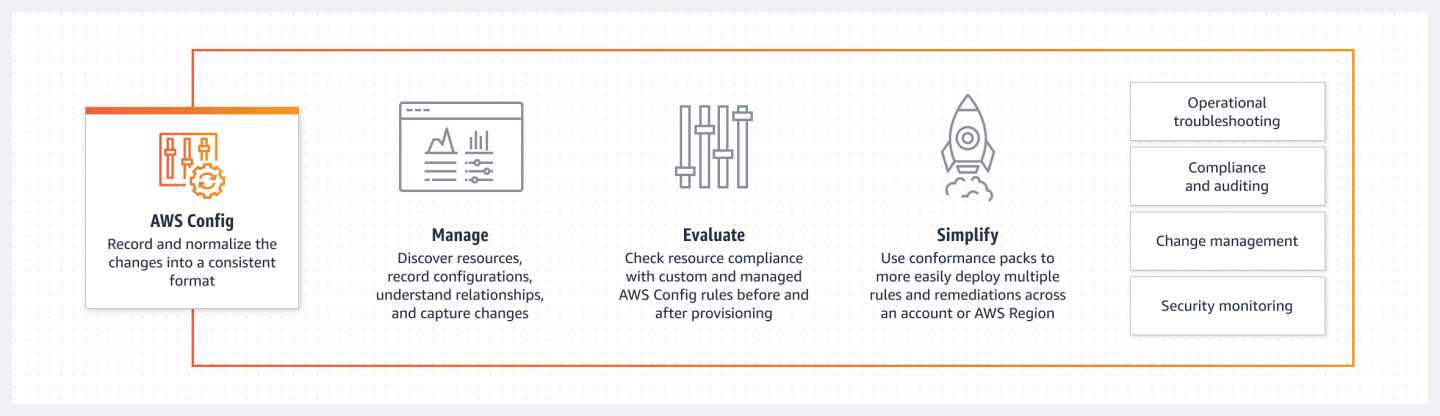
- Use one of the sample queries or write your own query by referring to the configuration schema of the AWS resource.

  For more information, see Querying the Current Configuration State of AWS Resources .

## How AWS Config Works

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. This includes how the resources are related to one another and how they were configured in the past so that you can see how the configurations and relationships change over time.

An AWS *resource* is an entity you can work with in AWS, such as an Amazon Elastic Compute Cloud (EC2) instance, an Amazon Elastic Block Store (EBS) volume, a security group, or an Amazon Virtual Private Cloud (VPC). For a complete list of AWS resources supported by AWS Config, see Supported Resource Types for AWS Config.



## Resource Discovery

When you turn on AWS Config, it first discovers the supported AWS resources that exist in your account and generates a configuration item for each resource.

AWS Config also generates configuration items when the configuration of a resource changes, and it maintains historical records of the configuration items of your resources from the time you start the configuration recorder. By default, AWS Config creates configuration items for every supported resource in the region. If you don't want AWS Config to create configuration items for all supported resources, you can specify the resource types that you want it to track.

Before specifying a resource type for AWS Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the AWS Region where you are setting up AWS Config. If a resource type is supported by AWS Config in at least one Region, you can enable the recording of that resource type in all Regions supported by AWS Config, even if the specified resource type is not supported the AWS Region where you are setting up AWS Config.

## Resource Tracking

AWS Config keeps track of all changes to your resources by invoking the Describe or the List API call for each resource in your account. The service uses those same API calls to capture configuration details for all related resources.

For example, removing an egress rule from a VPC security group causes AWS Config to invoke a Describe API call on the security group. AWS Config then invokes a Describe API call on all of the instances associated with the security group. The updated configurations of the security group (the resource) and of each instance (the related resources) are recorded as configuration items and delivered in a configuration stream to an Amazon Simple Storage Service (Amazon S3) bucket.

AWS Config also tracks the configuration changes that were not initiated by the API. AWS Config examines the resource configurations periodically and generates configuration items for the configurations that have changed.

If you are using AWS Config rules, AWS Config continuously evaluates your AWS resource configurations for desired settings. Depending on the rule, AWS Config will evaluate your resources either in response to configuration changes or periodically. Each rule is associated with an AWS Lambda function, which contains the evaluation logic for the rule. When AWS Config evaluates your resources, it invokes the rule's AWS Lambda function. The function returns the compliance status of the evaluated resources. If a resource violates the conditions of a rule, AWS Config flags

the resource and the rule as noncompliant. When the compliance status of a resource changes, AWS Config sends a notification to your Amazon SNS topic.

## Delivery of Configuration Items

AWS Config can deliver configuration items through one of the following channels:

### Amazon S3 Bucket

AWS Config tracks changes in the configuration of your AWS resources, and it regularly sends updated configuration details to an Amazon S3 bucket that you specify. For each resource type that AWS Config records, it sends a *configuration history file* every six hours. Each configuration history file contains details about the resources that changed in that six-hour period. Each file includes resources of one type, such as Amazon EC2 instances or Amazon EBS volumes. If no configuration changes occur, AWS Config does not send a file.

AWS Config sends a *configuration snapshot* to your Amazon S3 bucket when you use the deliver-config-snapshot command with the AWS CLI, or when you use the DeliverConfigSnapshot action with the AWS Config API. A configuration snapshot contains configuration details for all resources that AWS Config records in your AWS account. The configuration history file and configuration snapshot are in JSON format.

> **Note**
>
> AWS Config only delivers the configuration history files and configuration snapshots to the specified S3 bucket; AWS Config doesn't modify the lifecycle policies for objects in the S3 bucket. You can use lifecycle policies to specify whether you want to delete or archive objects to Amazon Glacier. For more information, see Managing Lifecycle Configuration in the *Amazon Simple Storage Service User Guide*. You can also see the Archiving Amazon S3 Data to Amazon Glacier blog post.

### Amazon SNS Topic

An Amazon Simple Notification Service (Amazon SNS) topic is a communication channel that Amazon SNS uses to deliver messages (or *notifications*) to subscribing endpoints such as an email address or clients. Other types of Amazon SNS notifications include push notification messages to apps on mobile phones, Short Message Service (SMS) notifications to SMS-enabled mobile phones

and smart phones, and HTTP POST requests. For best results, use Amazon SQS as the notification endpoint for the SNS topic and then process the information in the notification programmatically.

AWS Config uses the Amazon SNS topic that you specify to send you notifications. The type of notification that you are receiving is indicated by the value for the `messageType` key in the message body, as in the following example:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

The notifications can be any of the following message types.

| Message type | Description |
| --- | --- |
| ComplianceChangeNotification | The compliance type of a resource that AWS Config evaluates has changed. The compliance type indicates whether the resource complies with a specific AWS Config rule, and it is represented by the `ComplianceType` key in the message. The message includes `newEvaluationResult` and `oldEvaluationResult` objects for comparison. |
| ConfigRulesEvaluationStarted | AWS Config started evaluating your rule against the specified resources. |
| ConfigurationSnapshotDeliveryStarted | AWS Config started delivering the configuration snapshot to your Amazon S3 bucket. The name of the Amazon S3 bucket is provided for the `s3Bucket` key in the message. |
| ConfigurationSnapshotDeliveryCompleted | AWS Config successfully delivered the configuration snapshot to your Amazon S3 bucket. |
| ConfigurationSnapshotDeliveryFailed | AWS Config failed to deliver the configuration snapshot to your Amazon S3 bucket. |

| Message type | Description |
| --- | --- |
| ConfigurationHistoryDeliveryCompleted | AWS Config successfully delivered the configuration history to your Amazon S3 bucket. |
| ConfigurationItemChangeNotification | A resource has been created, deleted, or changed in configuration. This message includes the details of the configuration item that AWS Config creates for this change, and it includes the type of change. These notificat ions are delivered within minutes of a change and are collectively known as the *configura tion stream*. |
| OversizedConfigurationItemChangeNoti fication | This message type is delivered when a configuration item change notification exceeded the maximum size allowed by Amazon SNS. The message includes a summary of the configuration item. With the exception of SMS messages, Amazon SNS messages can contain up to 256 KB of text data, including XML, JSON, and unformatted text. You can view the complete notification in the specified Amazon S3 bucket location. |
| OversizedConfigurationItemChangeDeli veryFailed | AWS Config failed to deliver the oversized configuration item change notification to your Amazon S3 bucket. |

For example notifications, see Notifications that AWS Config Sends to an Amazon SNS topic. For more information about Amazon SNS, see the Amazon Simple Notification Service Developer Guide.

> **Note**
>
> **Why can't I see my latest configuration changes?**

AWS Config usually records configuration changes to your resources right after a change is detected, or at the frequency that you specify. However, this is on a best effort basis and can take longer at times. If issues persist after sometime, contact Support and provide your AWS Config metrics that are supported by Amazon CloudWatch. For information about these metrics, see AWS Config Usage and Success Metrics.

## Control Access to AWS Config

AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions.

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

  Create a permission set. Follow the instructions in Create a permission set in the *AWS IAM Identity Center User Guide*.
- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Create a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Create a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

# AWS Config terminology and concepts

To help you understand AWS Config, this topic explains some of the key concepts.

**Contents**


- AWS Config Interfaces
  - AWS Config Console
  - AWS Config CLI

- AWS Config APIs
  - AWS Config SDKs
- Resource Management
  - AWS Resources
  - Resource Relationship
- Configuration Recorder
- Delivery Channel
  - Configuration Items
  - Configuration History
  - Configuration Snapshot
  - Configuration Stream
- AWS Config Rules
  - Evaluation Results
  - Rule Types
  - Trigger Types
  - Evaluation modes
- Conformance Packs
- Multi-Account Multi-Region Data Aggregation
  - Source Account
  - Source Region
  - Aggregator
  - Service-linked aggregator
  - Aggregator Account
  - Authorization

# AWS Config Interfaces

## AWS Config Console

You can manage the service using the AWS Config console. For more information about the AWS Management Console, see AWS Management Console.

### AWS Config CLI

The AWS Command Line Interface is a unified tool that you can use to interact with AWS Config from the command line. For more information, see the AWS Command Line Interface User Guide. For a complete list of AWS Config CLI commands, see Available Commands.

### AWS Config APIs

In addition to the console and the CLI, you can also use the AWS Config RESTful APIs to program AWS Config directly. For more information, see the AWS Config API Reference.

### AWS Config SDKs

As an alternative to using the AWS Config API, you can use one of the AWS SDKs. Each SDK consists of libraries and sample code for various programming languages and platforms. The SDKs provide a convenient way to create programmatic access to AWS Config. For example, you can use the SDKs to sign requests cryptographically, manage errors, and retry requests automatically. For more information, see the Tools for Amazon Web Services page.

## Resource Management

Understanding the basic components of AWS Config will help you track resource inventory and changes and evaluate configurations of your AWS resources.

### AWS Resources

*AWS resources* are entities that you create and manage using the AWS Management Console, the AWS Command Line Interface (CLI), the AWS SDKs, or AWS partner tools. Examples of AWS resources include Amazon EC2 instances, security groups, Amazon VPCs, and Amazon Elastic Block Store. AWS Config refers to each resource using its unique identifier, such as the resource ID or an Amazon Resource Name (ARN). For a list of resource types that AWS Config supports, see Supported Resource Types for AWS Config.

### Resource Relationship

AWS Config discovers AWS resources in your account and then creates a map of relationships between AWS resources. For example, a relationship might include an Amazon EBS volume `vol-123ab45d` attached to an Amazon EC2 instance `i-a1b2c3d4` that is associated with security group `sg-ef678hk`.

For more information, see Supported Resource Types for AWS Config.

## Configuration Recorder

The *configuration recorder* stores the configuration changes to the resource types in scope as configuration items. For more information, see Working with the configuration recorder.

There are two types of configuration recorders.

| Type | Description |
| --- | --- |
| Customer managed configuration recorder | A configuration recorder that you managed. The resource types in scope are set by you. By default, a customer managed configuration recorder records all supported resources in the AWS Region where AWS Config is running. |
| Service-linked configuration recorder | A configuration recorder that is linked to a specific AWS service. The resource types in scope are set by the linked service. |

## Delivery Channel

As AWS Config continually records the changes that occur to your AWS resources, it sends notifications and updated configuration states through the *delivery channel*. You can manage the delivery channel to control where AWS Config sends configuration updates.

### Configuration Items

A *configuration item* represents a point-in-time view of the various attributes of a supported AWS resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if AWS Config is recording Amazon S3 buckets, AWS Config creates a configuration item whenever a bucket is created, updated, or deleted. You can also select for AWS Config to create a configuration item at the recording frequency that you set.

For more information, see Components of a Configuration Item and Recording Frequency.

## Configuration History

A *configuration history* is a collection of the configuration items for a given resource over any time period. A configuration history can help you answer questions about, for example, when the resource was first created, how the resource has been configured over the last month, and what configuration changes were introduced yesterday at 9 AM. The configuration history is available to you in multiple formats. AWS Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify. You can select a given resource in the AWS Config console and navigate to all previous configuration items for that resource using the timeline. Additionally, you can access the historical configuration items for a resource from the API.

For more information, see Viewing Compliance History and Querying Compliance History.

## Configuration Snapshot

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the AWS Config console and navigate through the snapshot of configuration items using the relationships between the resources.

For more information, see Delivering Configuration Snapshots, Viewing Configuration Snapshots, and Example Configuration Snapshot.

## Configuration Stream

A *configuration stream* is an automatically updated list of all configuration items for the resources that AWS Config is recording. Every time a resource is created, modified, or deleted, AWS Config creates a configuration item and adds to the configuration stream. The configuration stream works by using an Amazon Simple Notification Service (Amazon SNS) topic of your choice. The configuration stream is helpful for observing configuration changes as they occur so that you can spot potential problems, generating notifications if certain resources are changed, or updating external systems that need to reflect the configuration of your AWS resources.

# AWS Config Rules

An AWS Config rule is a compliance check that helps you manage your ideal configuration settings for specific AWS resources. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

## Evaluation Results

There are four possible evaluation results for an AWS Config rule.

| Evaluation result | Description |
| --- | --- |
| `COMPLIANT` | The rule passes the conditions of the compliance check. |
| `NON_COMPLIANT` | The rule fails the conditions of the compliance check. |
| `ERROR` | The one of the required/optional parameter s is not valid, not of the correct type, or is formatted incorrectly. |
| `NOT_APPLICABLE` | Used to filter out resources that the logic of the rule cannot be applied to. For example, the alb-desync-mode-check rule only checks Application Load Balancers, and ignores Network Load Balancers and Gateway Load Balancers. |

## Rule Types

There are two types of rules. For more information about the structure of rule definitions and rule metadata, see Components of an AWS Config Rule.

| Type | Description | More information |
| --- | --- | --- |
| Managed rules | Predefined, customizable rules created by AWS Config. | For a list of managed rules, see List of AWS Config Managed Rules. |
| Custom rules | Rules that you create from scratch. There are two ways to create AWS Config custom rules: Lambda functions (AWS Lambda Developer Guide) and Guard (Guard GitHub Repository) | For more information, see Creating AWS Config Custom Policy Rules and Creating AWS Config Custom Lambda Rules. |

## Trigger Types

After you add a rule to your account, AWS Config compares your resources to the conditions of the rule. After this initial evaluation, AWS Config continues to run evaluations each time one is triggered. The evaluation triggers are defined as part of the rule, and they can include the following types.

| Trigger type | Description |
| --- | --- |
| Configuration changes | AWS Config runs evaluations for the rule when there is a resource that matches the rule's scope and there is a change in configuration of the resource. The evaluation runs after AWS Config sends a configuration item change notification.<br><br>You choose which resources initiate the evaluation by defining the rule's *scope*. The scope can include the following:<br><br>• One or more resource types<br>• A combination of a resource type and a resource ID |

| Trigger type | Description |
| --- | --- |
| | • A combination of a tag key and value<br>• When any recorded resource is created, updated, or deleted<br><br>AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to define which resources initiate evaluations. |
| Periodic | AWS Config runs evaluations for the rule at a frequency that you choose; for example, every 24 hours. |
| Hybrid | Some rules have both configuration change and periodic triggers. For these rules, AWS Config evaluates your resources when it detects a configuration change and also at the frequency that you specify. |

## Evaluation modes

There are two evaluation modes for AWS Config rules.

| Evaluation mode | Description |
| --- | --- |
| Proactive | Use proactive evaluation to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.<br><br>For more information, see Evaluation modes. For a list of managed rules that support |

| Evaluation mode | Description |
| --- | --- |
| | proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode. |
| Detective | Use detective evaluation to evaluate resources that have already been deployed. This allows you to evaluate the configuration settings of your existing resources. |

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

## Conformance Packs

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.

Conformance packs are created by authoring a YAML template that contains the list of AWS Config managed or custom rules and remediation actions. You can deploy the template by using the AWS Config console or the AWS CLI.

To quickly get started and to evaluate your AWS environment, use one of the sample conformance pack templates. You can also create a conformance pack YAML file from scratch based on Custom Conformance Pack. A custom conformance pack is a unique collection of AWS Config rules and remediation actions that you can deploy together in an account and an AWS Region, or across an organization in AWS Organizations.

**Process checks** is a type of AWS Config rule that allows you to track your external and internal tasks that require verification as part of the conformance packs. These checks can be added to an existing conformance pack or a new conformance pack. You can track all compliance that includes AWS Configurations and manual checks in a single location.

# Multi-Account Multi-Region Data Aggregation

Multi-account multi-region data aggregation in AWS Config allows you to aggregate AWS Config configuration and compliance data from multiple accounts and regions into a single account. Multi-account multi-region data aggregation is useful for central IT administrators to monitor compliance for multiple AWS accounts in the enterprise. Using aggregators does not incur any additional costs.

## Source Account

A source account is the AWS account from which you want to aggregate AWS Config resource configuration and compliance data. A source account can be an individual account or an organization in AWS Organizations. You can provide source accounts individually or you can retrieve them through AWS Organizations.

## Source Region

A source region is the AWS Region from which you want to aggregate AWS Config configuration and compliance data.

## Aggregator

An aggregator collects AWS Config configuration and compliance data from multiple source accounts and regions. Create an aggregator in the region where you want to see the aggregated AWS Config configuration and compliance data.

> **Note**
>
> Aggregators provide a *read-only view* into the source accounts and regions that the aggregator is authorized to view by replicating data from the source accounts into the aggregator account. Aggregators do not provide mutating access into a source account or region. For example, this means that you cannot deploy rules through an aggregator or push snapshot files to a source account or region through an aggregator.

## Service-linked aggregator

A service-linked aggregator is linked to a specific AWS service. The configuration and compliance data in scope are set by the linked service.

### Aggregator Account

An aggregator account is an account where you create an aggregator.

### Authorization

As a source account owner, authorization refers to the permissions you grant to an aggregator account and region to collect your AWS Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of AWS Organizations.

# AWS Service Integrations with AWS Config

AWS Config supports integrations with several other AWS services. This list is non-exhaustive.

## AWS Organizations

You can use AWS Organizations to define the accounts to use for AWS Config's multi-account, multi-Region data aggregation capability. AWS Organizations is an account management service that helps you consolidate multiple AWS accounts into an organization that you create and centrally manage. By providing your AWS Organizations details, you can monitor the compliance status across your organization. For more information, AWS Config and AWS Organizations in the *AWS Organizations User Guide*.

## AWS Control Tower

AWS Control Tower enables AWS Config on all enrolled accounts, so that it can monitor compliance through detective controls, record resource changes, and deliver resource change logs to the log archive account. For more information, see Monitor resource changes with AWS Config in the *AWS Control Tower User Guide*.

## AWS CloudTrail

AWS Config integrates with AWS CloudTrail to correlate configuration changes to particular events in your account. You can use the CloudTrail logs to obtain the details of the event that invoked the change, including who made the request, at what time, and from which IP address. You can navigate to the AWS Config timeline from the CloudTrail console to view the configuration changes related to your AWS API activities.

For more information, see Logging AWS Config API Calls with AWS CloudTrail in the *AWS Config Developer Guide* and Create an event data store for AWS Config configuration items with the console in the *AWS CloudTrail User Guide*.

## AWS Security Hub CSPM

AWS Security Hub CSPM centralizes security checks from other AWS services, including AWS Config rules. Security Hub enables and controls AWS Config rules to verify your resource configurations are aligned to best practices. Enable AWS Config on all accounts in all Regions where Security Hub CSPM is to run security checks on your environment's resources. For more information, see AWS services that send findings to Security Hub in the *AWS Security Hub CSPM User Guide*.

> **Some Security Hub CSPM-related rules are periodic and do not depend on configuration items**
>
> Some Security Hub CSPM-related rules are periodic. These rule can run without the configuration recorder being enabled and do not depend on configuration items (CI). This means that if you view the rule page, there is no listed CI or supported resource. If you select the resource ID, you will see the following error: `The provided resource ID and resource type cannot be found`. This is expected behavior.

## AWS Trusted Advisor

AWS Config managed rules power a set of Trusted Advisor checks across all categories. When you enable certain managed rules, the corresponding Trusted Advisor checks are automatically enabled. To see which Trusted Advisor checks are powered by specific AWS Config managed rules, see AWS Trusted Advisor check reference in the *AWS Support User Guide*.

The AWS Config powered checks are available to customers with AWS Business Support, AWS Enterprise On-Ramp, and AWS Enterprise Support plans. If you enable AWS Config and you have one of these AWS Support plans, then you automatically see recommendations powered by corresponding deployed AWS Config managed rules.

> **Refresh requests are not allowed and resources cannot be excluded**
>
> Results for these checks are automatically refreshed based on change-triggered updates to AWS Config managed rules. Refresh requests are not allowed. Currently, you can't exclude resources from these checks.

For more information, see View Trusted Advisor checks powered by AWS Config in the *AWS Support User Guide*.

## AWS Audit Manager

You can use Audit Manager to capture AWS Config evaluations as evidence for audits. When you create or edit a custom control, you can specify one or more AWS Config rules as a data source mapping for evidence collection. AWS Config performs compliance checks based on these rules, and Audit Manager reports the results as compliance check evidence. For more information, see AWS Config Rules supported by AWS Audit Manager in the *AWS Audit Manager User Guide*.

## AWS Systems Manager

AWS Config integrates with Systems Manager to record configuration changes to software on your Amazon EC2 instances and servers in your on-premises environment. With this integration, you can gain visibility into operating system (OS) configurations, system-level updates, installed applications, network configuration, and more. AWS Config also provides a history of OS and system-level configuration changes alongside infrastructure configuration changes recorded for Amazon EC2 instances. You can navigate to the AWS Config timeline from the Systems Manager console to view the configuration changes of your managed Amazon EC2 instances. You can use AWS Config to view Systems Manager inventory history and track changes for all your managed instances.

For more information, see Integration with AWS services | Management and Governance, AWS Config configuration recorder, and AWS Config conformance pack deployment in the *AWS Systems Manager User Guide*.

## AWS Firewall Manager

To use Firewall Manager, you must enable AWS Config for each of your AWS Organizations member accounts. When new applications are created, Firewall Manager is the single service to build

firewall rules, create security policies, and enforce them consistently. For more information, see Enable AWS Config in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

> **Note**
>
> Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous. For more information on continuous recording and daily recording, see Recording Frequency.

## Amazon EC2 Dedicated Hosts

AWS Config integrates with Amazon EC2 Dedicated Hosts to assess license compliance. AWS Config records when instances are launched, stopped, or shut down on a Dedicated Host, and pairs this information with host and instance level information relevant to software licensing, such as Host ID, Amazon Machine Image (AMI) IDs, number of sockets, and physical cores. This helps you use AWS Config as a data source for your license reporting. You can navigate to the AWS Config timeline from the Amazon EC2 Dedicated Hosts console to view the configuration changes of your Amazon EC2 Dedicated Hosts.

For more information, see Track configuration changes in the *Amazon Elastic Compute Cloud User Guide for Linux Instances* or Track configuration changes in the *Amazon Elastic Compute Cloud User Guide for Windows Instances*.

## Application Load Balancers

AWS Config integrates with the Elastic Load Balancing (ELB) service to record configuration changes to Application Load Balancers. AWS Config also includes relationships with associated Amazon EC2 security groups, VPCs, and subnets. You can use this information for security analysis and troubleshooting. For example, you can check which security groups are associated with your Application Load Balancer at any point in time. You can navigate to the AWS Config timeline from the ELB console to view the configuration changes of your Application Load Balancers.

## AWS CodeBuild

AWS Configprovides an inventory of your AWS resources and a history of configuration changes to these resources. AWS Config supports AWS CodeBuild; as an AWS resource, which means

the service can track your CodeBuild projects. For more information, see Use AWS Config with CodeBuild sample in the *AWS CodeBuild User Guide*.

## AWS X-Ray

AWS X-Ray integrates with AWS Config to record configuration changes made to your X-Ray encryption resources. You can use AWS Config to inventory X-Ray encryption resources, audit the X-Ray configuration history, and send notifications based on resource changes. For more information, see Tracking X-Ray encryption configuration changes with AWS Config in the *AWS X-Ray Developer Guide*.

## AWS Service Management Connector

The AWS Service Management Connector for ServiceNow can synchronize AWS Config data from multiple accounts and Regions using an Aggregator. For more information, see Integrating AWS Config in ServiceNow in the *AWS Service Management Connector Administrator Guide*.

## Amazon API Gateway

You can use AWS Config to record configuration changes made to your API Gateway API resources and send notifications based on resource changes. Maintaining a configuration change history for API Gateway resources is useful for operational troubleshooting, audit, and compliance use cases. For more information, see Monitoring API Gateway API configuration with AWS Config in the *API Gateway Developer Guide*.

# Region Support for AWS Config

## Considerations

Some features of AWS Config are only supported in a subset of the AWS Regions where AWS Config is supported.

### Resource Management

- For a list of which AWS resource types are supported in which Regions, see Resource Coverage by Region Availability.

### AWS Config Rules

- For a list of which AWS Config rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.
- For a list of Regions which support the organizational deployment of AWS Config rules, see Organizational Rules | Region Support.

#### Conformance Packs

- For a list of Regions which support conformance packs and the organizational deployment of conformance packs, see Conformance Packs | Region Support.

#### Remediation

- For a list of Regions which support remediation actions for AWS Config rules, see Remediation Actions | Region Support.

#### Aggregators

- For a list of Regions which support the aggregators, see Aggregators | Region Support.

#### Advanced Queries

- For a list of Regions which support advanced queries, see Advanced Queries | Region Support.
- For a list of Regions which support the natural language query processor for advanced queries, see Natural language query processor for advanced queries | Region Support.

## List of Supported Regions

The following table lists the AWS Regions where you can enable AWS Config.

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS | |
| | | config-fips.us-east-2.amazonaws.com | HTTPS | |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com<br>config-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com<br>config-fips.us-west-1.amazonaws.com | HTTPS<br>HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com<br>config-fips.us-west-2.amazonaws.com | HTTPS<br>HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# Service Limits for AWS Config

The following table describes limits within AWS Config. Unless noted otherwise, the quotas can be increased upon request. You can request a quota increase.

For information about other limits in AWS, see AWS Service Limits.

### Resource tags

| Description | Limit Value | Can be increased |
| --- | --- | --- |
| Maximum number of tags per resource | 50 | No |

### AWS Config rules

| Description | Limit Value | Can be increased |
| --- | --- | --- |
| Maximum number of AWS Config Rules per Region per account | 1000 | No |

### Single Account Conformance Packs

| Description | Limit Value | Can be increased |
| --- | --- | --- |
| Maximum number of conformance packs per account | 50 | No |
| Maximum number of AWS Config Rules per conformance pack | 130 | No |

> **Note**
>
> AWS Config rules in conformance packs count in the limit for the Maximum number of AWS Config Rules per Region per account.

### Organization Conformance Packs

| Description | Limit Value | Can be increased |
| --- | --- | --- |
| Maximum number of conformance packs per organization | 50 | No |
| Maximum number of AWS Config Rules per organization conformance pack | 130 | No |

> **Note**
>
> Deploying at the organization level counts in the limit for child accounts. AWS Config rules in conformance packs count in the limit for the Maximum number of AWS Config Rules per Region per account.

### Aggregators

| Description | Limit Value | Can be increased |
| --- | --- | --- |
| Maximum number of configuration aggregators | 50 | Yes |
| Maximum number of accounts in an aggregator | 10000 | No |
| Maximum number of accounts added or deleted per week for all aggregators | 1000 | Yes |

> **Note**
>
> Organization level aggregators and individual account aggregators both count in the limit for the Maximum number of configuration aggregators.

### Advanced queries

| Description | Limit Value | Can be increased |
| --- | --- | --- |
| Maximum number of saved queries in a single account and a Region | 300 | Yes |

## Supplemental Information and Related Resources for AWS Config

The following related resources can help you as you work with this service.

- **AWS Config** – The primary web page for information about AWS Config.
- **AWS Config Pricing**
- **Technical FAQ**
- **AWS Config Rule Development Kit (RDK)** – An open-source tool that helps you set up AWS Config, author rules, and then test them using a variety of AWS resource types.
- **Partners** – Links to partner products that are fully integrated with AWS Config to help you visualize, monitor, and manage the data from your configuration stream, configuration snapshots, or configuration history.

- Classes & Workshops – Links to role-based and specialty courses, in addition to self-paced labs to help sharpen your AWS skills and gain practical experience.
- AWS Developer Center – Explore tutorials, download tools, and learn about AWS developer events.
- AWS Developer Tools – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.

- Getting Started Resource Center – Learn how to set up your AWS account, join the AWS community, and launch your first application.
- Hands-On Tutorials – Follow step-by-step tutorials to launch your first application on AWS.
- AWS Whitepapers – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- AWS Support Center – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- Support – The primary webpage for information about Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- Contact Us – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- AWS Site Terms – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.

## AWS Software Development Kits for AWS Config

An AWS software development kit (SDK) makes it easier to build applications that access cost-effective, scalable, and reliable AWS infrastructure services. With AWS SDKs, you can get started in minutes with a single, downloadable package that includes the library, code samples, and reference documentation. The following table lists the available SDKs and third-party libraries you can use to access AWS Config programmatically.

| Type of Access | Description |
| --- | --- |
| AWS SDKs | AWS provides the following SDKs:<br>• AWS SDK for C++ Documentation<br>• AWS Mobile SDK for iOS Documentation<br>• AWS SDK for Go Documentation<br>• AWS SDK for Java Documentation<br>• AWS SDK for JavaScript Documentation<br>• AWS SDK for .NET Documentation |

| Type of Access | Description |
| --- | --- |
| | • AWS SDK for PHP Documentation<br>• AWS SDK for Python (Boto) Documentation<br>• AWS SDK for Ruby Documentation |
| Third-party libraries | Developers in the AWS developer community also provide their own libraries, which you can find at the following AWS developer centers:<br>• AWS Java Developer Center<br>• AWS JavaScript Developer Center<br>• AWS PHP Developer Center<br>• AWS Python Developer Center<br>• AWS Ruby Developer Center<br>• AWS Windows and .NET Developer Center |

# Getting Started with AWS Config

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. With AWS Config, you can review changes in configurations and relationships between AWS resources, explore resource configuration history, and use rules to determine compliance. For more information, see What Is AWS Config? and How AWS Config Works.

## Signing up for AWS

**Topics**

- Sign up for an AWS account
- Create a user with administrative access

### Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

**To sign up for an AWS account**

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call or text message and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

# Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

### Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

### Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

### Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

**Assign access to additional users**

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.
2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

# Ways to Get Started with AWS Config

After you sign up for an AWS account, you can get started with AWS Config with the AWS Management Console, AWS CLI, or the AWS SDKs.

- Setting Up AWS Config with the Console
- Setting Up AWS Config with the AWS CLI
- Using AWS Config service with the AWS SDK

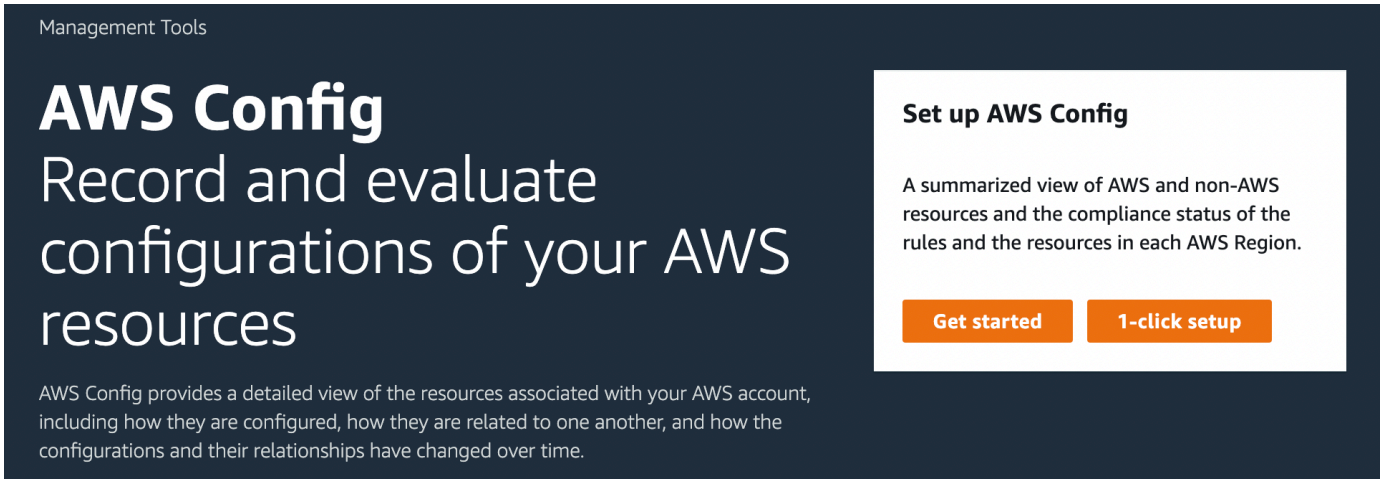
# Setting Up AWS Config with the Console

The AWS Management Console provides a quick and streamlined process for setting up AWS Config.

## Setting up

**To set up AWS Config with the console**

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. If this is the first time you are opening the AWS Config console or you are setting up AWS Config in a new region, the AWS Config console page looks like the following:




3. Choose **1-click setup** to launch AWS Config based on AWS best practices. You can also choose **Get started** to go through a more detailed setup process.

**Topics**

- 1-click setup for AWS Config
- Manual setup for AWS Config

## 1-click setup for AWS Config

AWS Config **1-click setup** helps simplify the getting started process for AWS Config console customers by reducing the number of manual selections. To go through all the manual selections of the setup process, see Manual setup.

**To set up AWS Config with the console using 1-click setup**

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **1-click setup**.

The set up page includes three steps, but through the **1-click setup** workflow, you are automatically directed to Step 3 (Review). The following provides a breakdown of that procedure.

- **Settings**: To select the manner by which the AWS Config console records resources and roles, and choose where configuration history and configuration snapshot files are sent.

- **Rules**: For AWS Regions that support AWS Config rules, this step is available for you to configure initial managed rules that you can add to your account. After setting up, AWS Config will evaluate your AWS resources against the rules that you chose. Additional rules can be created and existing ones can be updated in your account after setup.
- **Review**: To verify your setup details.

## Step 1: Settings

### Recording strategy

The option to record **All resource types with customizable overrides** is selected for you. AWS Config will record all current and future supported resource types in this Region. For more information, see Supported Resource Types.

- **Default settings**

  The default recording frequency is set to **Continuous** for you. This means AWS Config records configuration changes continuously whenever a change occurs.

  AWS Config also supports the option to set the recording frequency to **Daily**. If you select this option after setup, you will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded. For more information see, Recording Frequency.

  > **Note**
  >
  > AWS Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

- **Override settings – *optional***

  Optionally, after setup you can override the record frequency for specific resource types, or exclude specific resource types from recording. To override the default settings, choose **Settings** in the left navigation of the AWS Config console, and then choose **Edit**.

### Considerations When Recording Resources

### High Number of AWS Config Evaluations

You might notice increased activity in your account during your initial month recording with AWS Config when compared to subsequent months. During the initial bootstrapping process, AWS Config runs evaluations on all the resources in your account that you have selected for AWS Config to record.

If you are running ephemeral workloads, you may see increased activity from AWS Config as it records configuration changes associated with creating and deleting these temporary resources. An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and AWS Auto Scaling. If you want to avoid the increased activity from running ephemeral workloads, you can set up the configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with AWS Config turned off to avoid increased configuration recording and rule evaluations.

**Global resource types | Aurora global clusters are initially included in recording**

The `AWS::RDS::GlobalCluster` resource type will be recorded in all supported AWS Config Regions where the configuration recorder is enabled.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, you can exclude this resource type from recording after setup. Choose **Settings** in the left navigation bar, and then choosing **Edit**. From **Edit**, go to **Override settings** in the **Recording method** section, choose `AWS::RDS::GlobalCluster`, and choose the override "Exclude from recording".

**Global resource types | IAM resource types are initially excluded from recording**

"All globally recorded IAM resource types" are initially excluded from recording to help you reduce costs. This bundle includes IAM users, groups, roles, and customer managed policies. Choose **Remove** to remove the override and include these resources in your recording.

Additionally, the global IAM resource types (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy`) cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.

**Data governance**

The default data retention period to retain AWS Config data for 7 years (2557 days) is selected for you in this section.

The option to **Use an existing AWS Config service-linked role** is selected for you and set to the **AWS Config role**. Service-linked roles are predefined by AWS Config and include all the permissions that the service requires to call other AWS services.

**Delivery method**

The option to **Choose a bucket from your account** is selected for you in this section. This selection will default to the bucket in your account that is named in the format `config-bucket-accountid`. For example, `config-bucket-012345678901`. If you don't have a bucket created in that format, one will be created for you. If you want to create your own bucket, see Creating a bucket in the *Amazon Simple Storage Service User Guide*.

For more information about S3 buckets, see Buckets overview in the *Amazon Simple Storage Service User Guide*.

### Step 2: Rules

Under **AWS Managed Rules**, no rules are selected for you at this step. Instead, you are encouraged to create and update rules after you have finished setting up your account.

### Step 3: Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

## Manual setup for AWS Config

With the **Get started** workflow, you can go through all the manual selections of the setup process to get started with the AWS Config console. For a simplified getting started process, see 1-click setup.

**To set up AWS Config with the console using Get started**

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Get started**.

The setup page includes three steps. The following provides a breakdown of that procedure after you choose **Get started**.

- **Settings**: To select the manner by which the AWS Config console records resources and roles, and choose where configuration history and configuration snapshot files are sent.
- **Rules**: For AWS Regions that support AWS Config rules, this step is available for you to configure initial managed rules that you can add to your account. After setting up, AWS Config will evaluate your AWS resources against the rules that you chose. Additional rules can be created and existing ones can be updated and in your account after setup.
- **Review**: To verify your setup details.

## Step 1: Settings

### Recording strategy

In the **Recording method** section, choose a recording strategy. You can specify the AWS resources that you want AWS Config to record.

All resource types with customizable overrides

Set up AWS Config to record configuration changes for all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording. For more information, see Supported Resource Types.

- **Default settings**

  Configure the default recording frequency for all current and future supported resource types. For more information see, Recording Frequency.

  - Continuous recording – AWS Config will record configuration changes continuously whenever a change occurs.
  - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

> **Note**
>
> AWS Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

- **Override settings**

  Override the recording frequency for specific resource types, or exclude specific resource types from recording. If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

Specific resource types

Set AWS Config to record configuration changes for only the resource types that you specify.

- **Specific resource types**

  Choose a resource type to record and its frequency. For more information see, Recording Frequency.

  - Continuous recording – AWS Config will record configuration changes continuously whenever a change occurs.
  - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

  > **Note**
  >
  > AWS Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

  If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

### Considerations When Recording Resources

#### High Number of AWS Config Evaluations

You might notice increased activity in your account during your initial month recording with AWS Config when compared to subsequent months. During the initial bootstrapping process, AWS

Config runs evaluations on all the resources in your account that you have selected for AWS Config to record.

If you are running ephemeral workloads, you may see increased activity from AWS Config as it records configuration changes associated with creating and deleting these temporary resources. An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and AWS Auto Scaling. . If you want to avoid the increased activity from running ephemeral workloads, you can set up the configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with AWS Config turned off to avoid increased configuration recording and rule evaluations.

Considerations: All resource types with customizable overrides

**Globally recorded resource types | Aurora global clusters are initially included in recording**

The `AWS::RDS::GlobalCluster` resource type will be recorded in all supported AWS Config Regions where the configuration recorder is enabled.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, choose "AWS RDS GlobalCluster", and choose the override "Exclude from recording".

**Global resource types | IAM resource types are initially excluded from recording**

The global IAM resource types are initially excluded from recording to help you reduce costs. This bundle includes IAM users, groups, roles, and customer managed policies. Choose **Remove** to remove the override and include these resources in your recording.

Additionally, the global IAM resource types (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy`) cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.

**Limits**

You can add up to 100 frequency overrides and 600 exclusion overrides.

Daily recording cannot be specified for the following resource types:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`

- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

**Region Availability**

Before specifying a resource type for AWS Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the AWS Region where you set up AWS Config. If a resource type is supported by AWS Config in at least one Region, you can enable the recording of that resource type in all Regions supported by AWS Config, even if the specified resource type is not supported in the AWS Region where you set up AWS Config.

**Limits**

No limits if all resource types have the same frequency. You can add up to 100 resource types with Daily frequency if at least one resource type is set to Continuous.

The Daily frequency is not supported for the following resource types:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

**Data governance**

- For **Data retention period**, choose either the default retention period to retain AWS Config data for 7 years (2557) or set a custom rentention period for items recorded by AWS Config.

  AWS Config allows you to delete your data by specifying a retention period for your `ConfigurationItems`. When you specify a retention period, AWS Config retains your `ConfigurationItems` for that specified period. You can choose a period between a minimum of 30 days and a maximum of 7 years (2557 days). AWS Config deletes data older than your specified retention period.
- For **IAM role for AWS Config**, choose either an existing AWS Config service-linked role or an IAM role from your account.
  - Service-linked roles are predefined by AWS Config and include all the permissions that the service requires to call other AWS services.

> **Note**
>
> **Recommended: Use the Service-linked role**
> It is recommended that you use the service-linked role. A service-linked role adds all the necessary permissions for AWS Config to run as expected.

- Otherwise, choose an IAM role from one of your pre-existing roles and permission policies.

> **Note**
>
> **Policies and compliance results**
> IAM policies and other policies managed in AWS Organizations can impact whether AWS Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use AWS Config.
> **Keep Minimum Permisions When Reusing an IAM role**
> If you use an AWS service that uses AWS Config, such as AWS Security Hub CSPM or AWS Control Tower, and an IAM role has already been created, make sure that the IAM role that you use when setting up AWS Config keeps the same minimum permissions as the pre-existing IAM role. You must do this to ensure that the other AWS service continues to run as expected.
> For example, if AWS Control Tower has an IAM role that allows AWS Config to read S3 objects, make sure that the same permissions are granted to the IAM role you use when setting up AWS Config. Otherwise, it may interfere with how AWS Control Tower operates.

### Delivery method

- For **Delivery method**, choose the S3 bucket to which AWS Config sends configuration history and configuration snapshot files:
  - **Create a bucket** – For **S3 bucket name**, type a name for your S3 bucket.

    The name that you type must be unique across all existing bucket names in Amazon S3. One way to help ensure uniqueness is to include a prefix; for example, the name of your

organization. You can't change the bucket name after it is created. For more information, see Bucket Restrictions and Limitations in the *Amazon Simple Storage Service User Guide*.

- **Choose a bucket from your account** – For **S3 bucket name**, choose your preferred bucket.
- **Choose a bucket from another account** – For **S3 bucket name**, type the bucket name.

> **Note**
>
> **Bucket Permissions**
> If you choose a bucket from another account, that bucket must have policies that grant access permissions to AWS Config. For more information, see Permissions for the Amazon S3 Bucket for the AWS Config Delivery Channel.

- For **Amazon SNS topic**, choose **Stream configuration changes and notifications to an Amazon SNS topic** to have AWS Config send notifications such as configuration history delivery, configuration snapshot delivery, and compliance.
- If you chose to have AWS Config stream to an Amazon SNS topic, choose the target topic:
  - **Create a topic** – For **Topic Name**, type a name for your SNS topic.
  - **Choose a topic from your account** – For **Topic Name**, select your preferred topic.
  - **Choose a topic from another account** – For **Topic ARN**, type the Amazon Resource Name (ARN) of the topic. If you choose a topic from another account, the topic must have policies that grant access permissions to AWS Config. For more information, see Permissions for the Amazon SNS Topic.

> **Note**
>
> **Region for the Amazon SNS Topic**
> The Amazon SNS topic must exist in the same Region as the Region in which you set up AWS Config.

## Step 2: Rules

If you are setting up AWS Config in a Region that supports rules, choose **Next**.

### Step 3: Review

Review your AWS Config set up details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

### For more information

For information about looking up the existing resources in your account and understanding the configurations of your resources, see Looking up Resources, Viewing Compliance Informance, and Viewing Compliance History.

You can also use Amazon Simple Queue Service to monitor AWS resources programmatically. For more information, see Monitoring AWS Resource Changes with Amazon SQS.

## Setting Up AWS Config with the AWS CLI

The AWS CLI is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and use scripts to automate them. For more information about the AWS CLI and for instructions on installing the AWS CLI tools, see the following in the *AWS Command Line Interface User Guide*.

- AWS Command Line Interface User Guide
- Getting Set Up with the AWS Command Line Interface

If necessary, enter `aws configure` to configure the AWS CLI to use an AWS Region where AWS Config is available.

## Setting up

See the following topics to set up AWS Config with the AWS CLI.

**Topics**

- Prerequisites for Setting Up AWS Config with the AWS CLI
- Starting AWS Config with a customer managed configuration recorder using the AWS CLI
- Verifying that AWS Config is Successfully Started with the AWS CLI

# Prerequisites for Setting Up AWS Config with the AWS CLI

Before setting up AWS with the AWS CLI, you need to create an Amazon S3 bucket, an Amazon SNS topic, and an IAM role with attached policies as prerequisites. You can then use the AWS CLI to specify the bucket, topic, and role for AWS Config. Follow this procedure to set up your prerequisites for AWS Config.

**Topics**


- Step 1: Creating an Amazon S3 Bucket
- Step 2: Creating an Amazon SNS Topic
- Step 3: Creating an IAM Role


## Step 1: Creating an Amazon S3 Bucket

If you already have an Amazon S3 bucket in your account and want to use it, skip this step and go to Step 2: Creating an Amazon SNS Topic.

**Using the S3 console**

**To create a bucket**

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. Choose **Create bucket**.
3. In **Bucket name**, enter a DNS-compliant name for your bucket.

   The bucket name must:

   - Be unique across all of Amazon S3.
   - Be between 3 and 63 characters long.
   - Not contain uppercase characters.
   - Start with a lowercase letter or number.

   After you create the bucket, you can't change its name. Make sure the bucket name you choose is unique across all existing bucket names in Amazon S3. For more information on bucket naming rules and conventions, see Bucket restrictions and Limitations in the *Amazon Simple Storage Service User Guide*.

> **Important**
>
> Avoid including sensitive information in the bucket name. The bucket name is visible in the URLs that point to the objects in the bucket.

4. In **Region**, choose the AWS Region where you want the bucket to reside.

   Choose a Region close to you to minimize latency and costs and address regulatory requirements. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region. For a list of Amazon S3 AWS Regions, see AWS service endpoints in the *Amazon Web Services General Reference*.

5. In **Bucket settings for Block Public Access**, choose the Block Public Access settings that you want to apply to the bucket.

   We recommend that you leave all settings enabled unless you know you need to turn one or more of them off for your use case, such as to host a public website. Block public access settings that you enable for the bucket will also be enabled for all access points that you create on the bucket. For more information about blocking public access, see Using Amazon S3 Block Public Access in the *Amazon Simple Storage Service User Guide*.

6. (Optional) If you want to enable S3 Object Lock:

   a. Choose **Advanced settings**, and read the message that appears.

   > **Important**
   >
   > You can only enable S3 Object Lock for a bucket when you create it. If you enable Object Lock for the bucket, you can't disable it later. Enabling Object Lock also enables versioning for the bucket. After you enable Object Lock for the bucket, you must configure the Object Lock settings before any objects in the bucket will be protected. For more information about configuring protection for objects, see Configuring S3 Object Lock using the Amazon S3 console.

   b. If you want to enable Object Lock, enter *enable* in the text box and choose **Confirm**.

   For more information about the S3 Object Lock feature, see Locking Objects Using Amazon S3 Object Lock in the *Amazon Simple Storage Service User Guide*.

7. Choose **Create bucket**.

### Using the AWS SDKs

When you use the AWS SDKs to create a bucket, you must create a client and then use the client to send a request to create a bucket. As a best practice, you should create your client and bucket in the same AWS Region. If you don't specify a Region when you create a client or a bucket, Amazon S3 uses the default Region US East (N. Virginia).

To create a client to access a dual-stack endpoint, you must specify an AWS Region. For more information, see Amazon S3 dual-stack endpoints. For a list of available AWS Regions, see Regions and endpoints in the *AWS General Reference*.

When you create a client, the Region maps to the Region-specific endpoint. The client uses this endpoint to communicate with Amazon S3: `s3.<region>.amazonaws.com`. If your Region launched after March 20, 2019, your client and bucket must be in the same Region. However, you can use a client in the US East (N. Virginia) Region to create a bucket in any Region that launched before March 20, 2019. For more information, see Legacy Endpoints.

These AWS SDK code examples perform the following tasks:

- **Create a client by explicitly specifying an AWS Region** — In the example, the client uses the `s3.us-west-2.amazonaws.com` endpoint to communicate with Amazon S3. You can specify any AWS Region. For a list of AWS Regions, see Regions and endpoints in the *AWS General Reference*.
- **Send a create bucket request by specifying only a bucket name** — The client sends a request to Amazon S3 to create the bucket in the Region where you created a client.
- **Retrieve information about the location of the bucket** — Amazon S3 stores bucket location information in the *location* subresource that is associated with the bucket.

The following code examples show how to use `CreateBucket`.

.NET

**SDK for .NET**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

Create a bucket with object lock enabled.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- For API details, see CreateBucket in *AWS SDK for .NET API Reference*.

Bash

### AWS CLI with Bash script

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
```

```
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi
```

```
  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- For API details, see CreateBucket in *AWS CLI Command Reference*.

C++

**SDK for C++**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
bool AwsDoc::S3::createBucket(const Aws::String &bucketName,
                              const Aws::S3::S3ClientConfiguration &clientConfig)
 {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: createBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    } else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- For API details, see CreateBucket in *AWS SDK for C++ API Reference*.

## CLI

### AWS CLI

#### Example 1: To create a bucket

The following `create-bucket` example creates a bucket named `amzn-s3-demo-bucket`:

```
aws s3api create-bucket \
```

```
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

Output:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

For more information, see Creating a bucket in the *Amazon S3 User Guide*.

**Example 2: To create a bucket with owner enforced**

The following `create-bucket` example creates a bucket named `amzn-s3-demo-bucket` that uses the bucket owner enforced setting for S3 Object Ownership.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Output:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

For more information, see Controlling ownership of objects and disabling ACLs in the *Amazon S3 User Guide*.

**Example 3: To create a bucket outside of the ``us-east-1`` region**

The following `create-bucket` example creates a bucket named `amzn-s3-demo-bucket` in the `eu-west-1` region. Regions outside of `us-east-1` require the appropriate `LocationConstraint` to be specified in order to create the bucket in the desired region.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Output:

```
{
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

For more information, see Creating a bucket in the *Amazon S3 User Guide*.

- For API details, see CreateBucket in *AWS CLI Command Reference*.

Go

**SDK for Go V2**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create a bucket with default configuration.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
```

```
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
  }
 }
 return err
}
```

Create a bucket with object locking and wait for it to exist.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// S3Actions wraps S3 service actions.
type S3Actions struct {
 S3Client  *s3.Client
 S3Manager *manager.Uploader
}



// CreateBucketWithLock creates a new S3 bucket with optional object locking
 enabled
// and waits for the bucket to exist before returning.
func (actor S3Actions) CreateBucketWithLock(ctx context.Context, bucket string,
 region string, enableObjectLock bool) (string, error) {
 input := &s3.CreateBucketInput{
  Bucket: aws.String(bucket),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 }

 if enableObjectLock {
  input.ObjectLockEnabledForBucket = aws.Bool(true)
 }

 _, err := actor.S3Client.CreateBucket(ctx, input)
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
```

```
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", bucket)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", bucket)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(actor.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(bucket)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", bucket)
  }
 }

 return bucket, err
}
```

- For API details, see CreateBucket in *AWS SDK for Go API Reference*.

Java

**SDK for Java 2.x**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create a bucket.

```
    /**
     * Creates an S3 bucket asynchronously.
     *
     * @param bucketName the name of the S3 bucket to create
     * @return a {@link CompletableFuture} that completes when the bucket is
 created and ready
```

```
     * @throws RuntimeException if there is a failure while creating the bucket
     */
    public CompletableFuture<Void> createBucketAsync(String bucketName) {
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .build();

        CompletableFuture<CreateBucketResponse> response =
getAsyncClient().createBucket(bucketRequest);
        return response.thenCompose(resp -> {
            S3AsyncWaiter s3Waiter = getAsyncClient().waiter();
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                .bucket(bucketName)
                .build();

            CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
                s3Waiter.waitUntilBucketExists(bucketRequestWait);
            return waiterResponseFuture.thenAccept(waiterResponse -> {
                waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                    logger.info(bucketName + " is ready");
                });
            });
        }).whenComplete((resp, ex) -> {
            if (ex != null) {
                throw new RuntimeException("Failed to create bucket", ex);
            }
        });
    }
```

Create a bucket with object lock enabled.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();
```

```
        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- For API details, see CreateBucket in *AWS SDK for Java 2.x API Reference*.

JavaScript

**SDK for JavaScript (v3)**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create the bucket.

```
import {
  BucketAlreadyExists,
  BucketAlreadyOwnedByYou,
  CreateBucketCommand,
  S3Client,
  waitUntilBucketExists,
} from "@aws-sdk/client-s3";

/**
 * Create an Amazon S3 bucket.
 * @param {{ bucketName: string }} config
 */
export const main = async ({ bucketName }) => {
  const client = new S3Client({});

  try {
    const { Location } = await client.send(
```

```
      new CreateBucketCommand({
        // The name of the bucket. Bucket names are unique and have several other
 constraints.
        // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
        Bucket: bucketName,
      }),
    );
    await waitUntilBucketExists({ client }, { Bucket: bucketName });
    console.log(`Bucket created with location ${Location}`);
  } catch (caught) {
    if (caught instanceof BucketAlreadyExists) {
      console.error(
        `The bucket "${bucketName}" already exists in another AWS account. Bucket
 names must be globally unique.`,
      );
    }
    // WARNING: If you try to create a bucket in the North Virginia region,
    // and you already own a bucket in that region with the same name, this
    // error will not be thrown. Instead, the call will return successfully
    // and the ACL on that bucket will be reset.
    else if (caught instanceof BucketAlreadyOwnedByYou) {
      console.error(
        `The bucket "${bucketName}" already exists in this AWS account.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- For more information, see AWS SDK for JavaScript Developer Guide.
- For API details, see CreateBucket in *AWS SDK for JavaScript API Reference*.

Kotlin

### SDK for Kotlin

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client.fromEnvironment { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- For API details, see CreateBucket in *AWS SDK for Kotlin API reference*.

PHP

### SDK for PHP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create a bucket.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
```

```
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
 $exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- For API details, see CreateBucket in *AWS SDK for PHP API Reference*.

## Python

### SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create a bucket with default settings.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
```

```
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

Create a versioned bucket with a lifecycle configuration.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.
```

```
    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
```

```
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- For API details, see CreateBucket in *AWS SDK for Python (Boto3) API Reference*.

Ruby

**SDK for Ruby**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
```

```
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- For API details, see CreateBucket in *AWS SDK for Ruby API Reference*.

Rust

**SDK for Rust**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

    // BucketAlreadyExists and BucketAlreadyOwnedByYou are not problems for this
 task.
    create.map(Some).or_else(|err| {
        if err
            .as_service_error()
            .map(|se| se.is_bucket_already_exists() ||
 se.is_bucket_already_owned_by_you())
            == Some(true)
        {
            Ok(None)
        } else {
            Err(S3ExampleError::from(err))
```

```
        }
    })
}
```

- For API details, see CreateBucket in *AWS SDK for Rust API reference*.

SAP ABAP

**SDK for SAP ABAP**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
    TRY.
        " determine our region from our session
        DATA(lv_region) = CONV /aws1/s3_bucketlocationcnstrnt( lo_session-
>get_region( ) ).
        DATA lo_constraint TYPE REF TO /aws1/cl_s3_createbucketconf.
        " When in the us-east-1 region, you must not specify a constraint
        " In all other regions, specify the region as the constraint
        IF lv_region = 'us-east-1'.
          CLEAR lo_constraint.
        ELSE.
          lo_constraint = NEW /aws1/cl_s3_createbucketconf( lv_region ).
        ENDIF.

        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
            io_createbucketconfiguration  = lo_constraint ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- For API details, see CreateBucket in *AWS SDK for SAP ABAP API reference*.

## Swift

### SDK for Swift

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import AWSS3

    public func createBucket(name: String) async throws {
        var input = CreateBucketInput(
            bucket: name
        )

        // For regions other than "us-east-1", you must set the
 locationConstraint in the createBucketConfiguration.
        // For more information, see LocationConstraint in the S3 API guide.
        // https://docs.aws.amazon.com/AmazonS3/latest/API/
API_CreateBucket.html#API_CreateBucket_RequestBody
        if let region = configuration.region {
            if region != "us-east-1" {
                input.createBucketConfiguration =
 S3ClientTypes.CreateBucketConfiguration(locationConstraint:
 S3ClientTypes.BucketLocationConstraint(rawValue: region))
            }
        }

        do {
            _ = try await client.createBucket(input: input)
        }
        catch let error as BucketAlreadyOwnedByYou {
            print("The bucket '\(name)' already exists and is owned by you. You
 may wish to ignore this exception.")
            throw error
        }
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
```

```
            throw error
        }
    }
```

- For API details, see CreateBucket in *AWS SDK for Swift API reference*.

> **Note**
>
> You can also use an Amazon S3 bucket from a different account, but you may need to create a policy for the bucket that grants access permissions to AWS Config. For information on granting permissions to an Amazon S3 bucket, see Permissions for the Amazon S3 Bucket for the AWS Config Delivery Channel, and then go to Step 2: Creating an Amazon SNS Topic.

## Step 2: Creating an Amazon SNS Topic

If you already have an Amazon SNS topic in your account and want to use it, skip this step and go to Step 3: Creating an IAM Role.

**Using the SNS console**

**To create an Amazon SNS topic**

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. Do one of the following:
   - If no topics have ever been created under your AWS account before, read the description of Amazon SNS on the home page.
   - If topics have been created under your AWS account before, on the navigation panel, choose **Topics**.
3. On the **Topics** page, choose **Create topic**.
4. On the **Create topic** page, in the **Details** section, do the following:
   a. For **Type**, choose a topic type (**Standard** or **FIFO**).
   b. Enter a **Name** for the topic. For a FIFO topic, add **.fifo** to the end of the name.

c. (Optional) Enter a **Display name** for the topic.

d. (Optional) For a FIFO topic, you can choose **content-based message deduplication** to enable default message deduplication. For more information, see Message deduplication for FIFO topics.

5. (Optional) Expand the **Encryption** section and do the following. For more information, see Encryption at rest.

   a. Choose **Enable encryption**.

   b. Specify the customer master key (CMK). For more information, see Key terms.

      For each CMK type, the **Description**, **Account**, and **CMK ARN** are displayed.

      > **Important**
      >
      > If you aren't the owner of the CMK, or if you log in with an account that doesn't have the `kms:ListAliases` and `kms:DescribeKey` permissions, you won't be able to view information about the CMK on the Amazon SNS console.
      > Ask the owner of the CMK to grant you these permissions. For more information, see the AWS KMS API Permissions: Actions and Resources Reference in the *AWS Key Management Service Developer Guide*.

      - The AWS managed CMK for Amazon SNS **(Default) alias/aws/sns** is selected by default.

        > **Note**
        >
        > Keep the following in mind:
        >
        > - The first time you use the AWS Management Console to specify the AWS managed CMK for Amazon SNS for a topic, AWS KMS creates the AWS managed CMK for Amazon SNS.
        > - Alternatively, the first time you use the `Publish` action on a topic with SSE enabled, AWS KMS creates the AWS managed CMK for Amazon SNS.

      - To use a custom CMK from your AWS account, choose the **Customer master key (CMK)** field and then choose the custom CMK from the list.

> **Note**
>
> For instructions on creating custom CMKs, see Creating Keys in the *AWS Key Management Service Developer Guide*

- To use a custom CMK ARN from your AWS account or from another AWS account, enter it into the **Customer master key (CMK)** field.

6. (Optional) By default, only the topic owner can publish or subscribe to the topic. To configure additional access permissions, expand the **Access policy** section. For more information, see Identity and access management in Amazon SNS and Example cases for Amazon SNS access control.

> **Note**
>
> When you create a topic using the console, the default policy uses the `aws:SourceOwner` condition key. This key is similar to `aws:SourceAccount`.

7. (Optional) To configure how Amazon SNS retries failed message delivery attempts, expand the **Delivery retry policy (HTTP/S)** section. For more information, see Amazon SNS message delivery retries.
8. (Optional) To configure how Amazon SNS logs the delivery of messages to CloudWatch, expand the **Delivery status logging** section. For more information, see Amazon SNS message delivery status.
9. (Optional) To add metadata tags to the topic, expand the **Tags** section, enter a **Key** and a **Value** (optional) and choose **Add tag**. For more information, see Amazon SNS topic tagging.
10. Choose **Create topic**.

    The topic is created and the ***MyTopic*** page is displayed.

    The topic's **Name**, **ARN**, (optional) **Display name**, and **Topic owner**'s AWS account ID are displayed in the **Details** section.
11. Copy the topic ARN to the clipboard, for example:

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

**To subscribe an email address to the Amazon SNS topic**

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v3/home.
2. In the left navigation pane, choose **Subscriptions**.
3. On the **Subscriptions** page, choose **Create subscription**.
4. On the **Create subscription** page, in the **Details** section, do the following:

   a. For **Topic ARN**, choose the Amazon Resource Name (ARN) of a topic.

   b. For **Protocol**, choose an endpoint type. The available endpoint types are:

      - HTTP/HTTPS
      - Email/Email-JSON
      - Amazon Data Firehose
      - Amazon SQS

      > **Note**
      >
      > To subscribe to an SNS FIFO topic, choose this option.

      - AWS Lambda
      - Platform application endpoint
      - SMS

   c. For **Endpoint**, enter the endpoint value, such as an email address or the ARN of an Amazon SQS queue.

   d. Firehose endpoints only: For **Subscription role ARN**, specify the ARN of the IAM role that you created for writing to Firehose delivery streams. For more information, see Prerequisites for subscribing Firehose delivery streams to Amazon SNS topics.

   e. (Optional) For Firehose, Amazon SQS, HTTP/S endpoints, you can also enable raw message delivery. For more information, see Amazon SNS raw message delivery.

   f. (Optional) To configure a filter policy, expand the **Subscription filter policy** section. For more information, see Amazon SNS subscription filter policies.

   g. (Optional) To configure a dead-letter queue for the subscription, expand the **Redrive policy (dead-letter queue)** section. For more information, see Amazon SNS dead-letter queues (DLQs).

   h. Choose **Create subscription**.

The console creates the subscription and opens the subscription's **Details** page.

### Using the AWS SDKs

To use an AWS SDK, you must configure it with your credentials. For more information, see The shared config and credentials files in the *AWS SDKs and Tools Reference Guide*.

The following code examples show how to use `CreateTopic`.

.NET

**SDK for .NET**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create a topic with a specific name.

```
using System;
using System.Threading.Tasks;
using Amazon.SimpleNotificationService;
using Amazon.SimpleNotificationService.Model;

/// <summary>
/// This example shows how to use Amazon Simple Notification Service
/// (Amazon SNS) to add a new Amazon SNS topic.
/// </summary>
public class CreateSNSTopic
{
    public static async Task Main()
    {
        string topicName = "ExampleSNSTopic";

        IAmazonSimpleNotificationService client = new
AmazonSimpleNotificationServiceClient();

        var topicArn = await CreateSNSTopicAsync(client, topicName);
        Console.WriteLine($"New topic ARN: {topicArn}");
```

```
        }

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Create a new topic with a name and specific FIFO and de-duplication attributes.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
```

```
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
 "true");
            }
        }

        var createResponse = await
 _amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- For API details, see CreateTopic in *AWS SDK for .NET API Reference*.

C++

**SDK for C++**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
```

```
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- For API details, see CreateTopic in *AWS SDK for C++ API Reference*.

## CLI

### AWS CLI

#### To create an SNS topic

The following `create-topic` example creates an SNS topic named `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Output:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

For more information, see Using the AWS Command Line Interface with Amazon SQS and Amazon SNS in the *AWS Command Line Interface User Guide*.

- For API details, see CreateTopic in *AWS CLI Command Reference*.

Go

**SDK for Go V2**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/sns"
 "github.com/aws/aws-sdk-go-v2/service/sns/types"
)
```

```
// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(ctx context.Context, topicName string,
 isFifoTopic bool, contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(ctx, &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- For API details, see CreateTopic in *AWS SDK for Go API Reference*.

Java

### SDK for Java 2.x

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- For API details, see CreateTopic in *AWS SDK for Java 2.x API Reference*.

JavaScript

**SDK for JavaScript (v3)**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create the client in a separate module and export it.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

Import the SDK and client modules and call the API.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- For more information, see AWS SDK for JavaScript Developer Guide.
- For API details, see CreateTopic in *AWS SDK for JavaScript API Reference*.

Kotlin

### SDK for Kotlin

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient.fromEnvironment { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- For API details, see CreateTopic in *AWS SDK for Kotlin API reference*.

PHP

### SDK for PHP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
use Aws\Sns\SnsClient;
```

```
/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- For more information, see AWS SDK for PHP Developer Guide.
- For API details, see CreateTopic in *AWS SDK for PHP API Reference*.

## Python

### SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- For API details, see CreateTopic in *AWS SDK for Python (Boto3) API Reference*.

## Ruby

### SDK for Ruby

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = 'YourTopicName' # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end
```

- For more information, see AWS SDK for Ruby Developer Guide.
- For API details, see CreateTopic in *AWS SDK for Ruby API Reference*.

Rust

### SDK for Rust

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- For API details, see CreateTopic in *AWS SDK for Rust API reference*.

SAP ABAP

### SDK for SAP ABAP

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
    TRY.
        oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
 is returned for testing purposes. "
        MESSAGE 'SNS topic created' TYPE 'I'.
      CATCH /aws1/cx_snstopiclimitexcdex.
```

```
        MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- For API details, see CreateTopic in *AWS SDK for SAP ABAP API reference*.

Swift

**SDK for Swift**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import AWSSNS

        let config = try await SNSClient.SNSClientConfiguration(region: region)
        let snsClient = SNSClient(config: config)

        let output = try await snsClient.createTopic(
            input: CreateTopicInput(name: name)
        )

        guard let arn = output.topicArn else {
            print("No topic ARN returned by Amazon SNS.")
            return
        }
```

- For API details, see CreateTopic in *AWS SDK for Swift API reference*.

> **Note**
>
> You can also use an Amazon SNS topic in a different account, but in that case you might need to create a policy for topic that grants access permissions to AWS Config. For

information on granting permissions to an Amazon SNS topic, see Permissions for the Amazon SNS Topic and then go to Step 3: Creating an IAM Role.

## Step 3: Creating an IAM Role

**Important**

**(Recommended) Use the AWS Config service-linked role**
It is recommended to use the AWS Config service-linked role: `AWSServiceRoleForConfig`. Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services. The AWS Config service-linked role is required for service-linked configuration recorders.
For more information, see Using Service-Linked Roles for AWS Config.

### Using the IAM console

You can use the IAM console to create an IAM role that grants AWS Config permissions to access your Amazon S3 bucket, access your Amazon SNS topic, and get configuration details for supported AWS resources. When you use the console to create an IAM role, AWS Config automatically attaches the required permissions to the role for you.

**Note**

If you have used an AWS service that uses AWS Config (such as AWS Security Hub or AWS Control Tower) and an AWS Config role has already been created, you should make sure that the IAM role you use when setting up AWS Config keeps the same minimum privileges as the already created AWS Config role in order for the other AWS service to continue to run as expected.
For example, if AWS Control Tower has an IAM role that allows AWS Config to read Amazon S3 objects, you should guarantee the same permissions are granted within the IAM role you use when setting up AWS Config. Otherwise, it may interfere with AWS Control Tower's operations.
For more information about IAM roles for AWS Config, see AWS Identity and Access Management.

**To create a role for an AWS service**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the IAM console, choose **Roles**, and then choose **Create role**.
3. For **Select trusted entity**, choose **AWS service**.
4. Choose the use case you want for AWS Config: **Config - Customizable**, **Config - Organizations**, **Config**, or **Config - Conformance Packs**. Then, choose **Next**.
5. On the **Name, review, and create** page, review the details about your role, and choose **Create Role**.

## Using the AWS SDKs

To use an AWS SDK, you must configure it with your credentials. For more information, see The shared config and credentials files in the *AWS SDKs and Tools Reference Guide*.

The following code examples show how to use `CreateRole`.

.NET

**SDK for .NET**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
```

```
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- For API details, see CreateRole in *AWS SDK for .NET API Reference*.

## Bash

### AWS CLI with Bash script

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
```

```
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_json -- The assume role policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
```

```
    usage
    return 1
  fi

  response=$(aws iam create-role \
    --role-name "$role_name" \
    --assume-role-policy-document "$policy_document" \
    --output text \
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- For API details, see CreateRole in *AWS CLI Command Reference*.

C++

### SDK for C++

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;
```

```
    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- For API details, see CreateRole in *AWS SDK for C++ API Reference*.

## CLI

### AWS CLI

#### Example 1: To create an IAM role

The following `create-role` command creates a role named `Test-Role` and attaches a trust policy to it.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Output:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
```

```
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

The trust policy is defined as a JSON document in the *Test-Role-Trust-Policy.json* file. (The file name and extension do not have significance.) The trust policy must specify a principal.

To attach a permissions policy to a role, use the `put-role-policy` command.

For more information, see Creating IAM roles in the *AWS IAM User Guide*.

**Example 2: To create an IAM role with specified maximum session duration**

The following `create-role` command creates a role named `Test-Role` and sets a maximum session duration of 7200 seconds (2 hours).

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

Output:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
```

```
            ]
        }
    }
}
```

For more information, see Modifying a role maximum session duration (AWS API) in the *AWS IAM User Guide*.

**Example 3: To create an IAM Role with tags**

The following command creates an IAM Role `Test-Role` with tags. This example uses the `--tags` parameter flag with the following JSON-formatted tags: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. Alternatively, the `--tags` flag can be used with tags in the shorthand format: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Output:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
```

```
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

For more information, see Tagging IAM roles in the *AWS IAM User Guide*.

- For API details, see CreateRole in *AWS CLI Command Reference*.

## Go

### SDK for Go V2

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 "github.com/aws/aws-sdk-go-v2/service/iam/types"
)

// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
```

```
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
   Effect:    "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action:    []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- For API details, see CreateRole in *AWS SDK for Go API Reference*.

Java

**SDK for Java 2.x**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
```

```
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
represents the trust policy.\s
               """;

       if (args.length != 2) {
           System.out.println(usage);
           System.exit(1);
       }

       String rolename = args[0];
       String fileLocation = args[1];
       Region region = Region.AWS_GLOBAL;
       IamClient iam = IamClient.builder()
               .region(region)
               .build();

       String result = createIAMRole(iam, rolename, fileLocation);
       System.out.println("Successfully created user: " + result);
       iam.close();
   }

   public static String createIAMRole(IamClient iam, String rolename, String
fileLocation) throws Exception {
       try {
           JSONObject jsonObject = (JSONObject)
readJsonSimpleDemo(fileLocation);
           CreateRoleRequest request = CreateRoleRequest.builder()
                   .roleName(rolename)
                   .assumeRolePolicyDocument(jsonObject.toJSONString())
                   .description("Created using the AWS SDK for Java")
                   .build();

           CreateRoleResponse response = iam.createRole(request);
           System.out.println("The ARN of the role is " +
response.role().arn());

       } catch (IamException e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
       return "";
   }
```

```
    public static Object readJsonSimpleDemo(String filename) throws Exception {
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- For API details, see CreateRole in *AWS SDK for Java 2.x API Reference*.

JavaScript

**SDK for JavaScript (v3)**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

Create the role.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
```

```
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- For API details, see CreateRole in *AWS SDK for JavaScript API Reference*.

PHP

**SDK for PHP**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
```

```
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- For API details, see CreateRole in *AWS SDK for PHP API Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example creates a new role named `MyNewRole` and attaches to it the policy found in the file `NewRoleTrustPolicy.json`. Note that you must use the `-Raw` switch parameter to successfully process the JSON policy file. The policy document displayed in the output is URL encoded. It is decoded in this example with the `UrlDecode` .NET method.**

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

**Output:**

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
```

```
                              %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                              %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                              %20%5D%0D%0A%7D
CreateDate                  : 4/15/2015 11:04:23 AM
Path                        : /
RoleId                      : V5PAJI2KPN4EAEXAMPLE1
RoleName                    : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- For API details, see CreateRole in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example creates a new role named `MyNewRole` and attaches to it the policy found in the file `NewRoleTrustPolicy.json`. Note that you must use the `-Raw` switch parameter to successfully process the JSON policy file. The policy document displayed in the output is URL encoded. It is decoded in this example with the `UrlDecode` .NET method.**

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

**Output:**

```
Arn                         : arn:aws:iam::123456789012:role/MyNewRole
```

```
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
RoleId                   : V5PAJI2KPN4EAEXAMPLE1
RoleName                 : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- For API details, see CreateRole in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

Python

### SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version":"2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- For API details, see CreateRole in *AWS SDK for Python (Boto3) API Reference*.

Ruby

**SDK for Ruby**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
     )
   end

   role_arn
 rescue Aws::IAM::Errors::ServiceError => e
   @logger.error("Error creating role: #{e.message}")
   nil
 end
```

- For API details, see CreateRole in *AWS SDK for Ruby API Reference*.

Rust

**SDK for Rust**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- For API details, see CreateRole in *AWS SDK for Rust API reference*.

Swift

### SDK for Swift

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
import AWSIAM
import AWSS3


    public func createRole(name: String, policyDocument: String) async throws ->
 String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- For API details, see CreateRole in *AWS SDK for Swift API reference*.

# Starting AWS Config with a customer managed configuration recorder using the AWS CLI

You can start AWS Config by creating a customer managed configuration recorder. To create a customer managed configuration recorder with the AWS CLI, use the following commands: `put-configuration-recorder`, `put-delivery-channel`, and `start-configuration-recorder`.

- The `put-configuration-recorder` command creates a customer managed configuration recorder.
- The `put-delivery-channel` command creates a delivery channel where AWS Config delivers configuration information to an S3 bucket and SNS topic.
- The `start-configuration-recorder` starts the customer managed configuration recorder. The customer managed configuration recorder will begin recording configuration changes for the resource types you specify.

**Topics**


- Considerations
- Step 1: Run the put-configuration-recorder
- Step 2: Run the put-delivery-channel command
- Step 3: Run the start-configuration-recorder command


## Considerations

### S3 bucket, SNS topic, and IAM role are required

To create a customer managed configuration recorder, you need to create an S3 bucket, an SNS topic, and an IAM role with attached policies as prerequisites. To set up your prerequisites for AWS Config, see Prerequisites.

### One customer managed configuration recorder per account per Region

You can have only one customer managed configuration recorder for each AWS account for each AWS Region.

### One delivery channel per account per Region

You can have only one delivery channel region for each AWS account for each AWS Region.

**Policies and compliance results**

IAM policies and other policies managed in AWS Organizations can impact whether AWS Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use AWS Config.

## Step 1: Run the put-configuration-recorder

Use the `put-configuration-recorder` command to create a customer managed configuration recorder:

This command uses the `--configuration-recorder` and `---recording-group` fields.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

### The `configuration-recorder` field

The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`). You can also use this field to override the recording frequency for specific resource types.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

### The `recording-group` field

The `recordingGroup.json` file specifies which resource types are recorded.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

For more information about these fields, see `put-configuration-recorder` in the *AWS CLI Command Reference*.

## Step 2: Run the put-delivery-channel command

Use the `put-delivery-channel` command to create a delivery channel:

This command uses the `--delivery-channel` field.

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

### The `delivery-channel` field

The `deliveryChannel.json` file specifies the following:

- The `name` for the delivery channel.
- The `s3BucketName` where AWS Config sends configuration snapshots.
- The `snsTopicARN` where AWS Config sends notifications
- The `configSnapshotDeliveryProperties` which sets how often AWS Config delivers configuration snapshots and how often it invokes evaluations for periodic rules.

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
```

```
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

For more information about these fields, see `put-delivery-channel` in the *AWS CLI Command Reference*.

### Step 3: Run the start-configuration-recorder command

Use the `start-configuration-recorder` command to start AWS Config:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

For more information about these fields, see `start-configuration-recorder` in the *AWS CLI Command Reference*.

## Verifying that AWS Config is Successfully Started with the AWS CLI

After you have started AWS Config, you can use AWS CLI commands to check that the AWS Config is running and that AWS Config has created a configuration recorder and a delivery channel. You can also confirm that AWS Config has started recording and delivering configurations to the delivery channel.

**Topics**


- Step 1: Check that a delivery channel is Created
- Step 2: Check that a configuration recorder is Created
- Step 3: Check that AWS Config has started recording


### Step 1: Check that a delivery channel is Created

Use the `describe-delivery-channels` command to check that your Amazon S3 bucket and Amazon SNS topic is configured.

You can use the `--delivery-channel-names` field to specify a list of delivery channel. If a delivery channel is not specified, this command returns the details of all delivery channels associated with the account.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

## Step 2: Check that a configuration recorder is Created

Use the `describe-configuration-recorders` command to check that a configuration recorder is created.

You can use the `arn` and `configuration-recorder-names` fields to specify a list of configuration recorders. If a configuration recorder is not specified, this command returns the details of all configuration recorders associated with the account.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

## Step 3: Check that AWS Config has started recording

Use the `describe-configuration-recorder-status` command to check that the configuration recorder is successfully recording the resource types in scope.

You can use the `arn` and `configuration-recorder-names` fields to specify a list of configuration recorders. If a configuration recorder is not specified, this command returns the details of all configuration recorders associated with the account.

```
$ aws configservice describe-configuration-recorder-status
```

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

The `true` value in the `recording` field confirms that the configuration recorder has started recording configurations. AWS Config records the time in UTC. The output is displayed as a Unix timestamp.

## Using AWS Config with an AWS SDK

AWS software development kits (SDKs) are available for many popular programming languages. Each SDK provides an API, code examples, and documentation that make it easier for developers to build applications in their preferred language.

| SDK documentation | Code examples |
| --- | --- |
| AWS SDK for C++ | AWS SDK for C++ code examples |
| AWS CLI | AWS CLI code examples |
| AWS SDK for Go | AWS SDK for Go code examples |
| AWS SDK for Java | AWS SDK for Java code examples |
| AWS SDK for JavaScript | AWS SDK for JavaScript code examples |
| AWS SDK for Kotlin | AWS SDK for Kotlin code examples |
| AWS SDK for .NET | AWS SDK for .NET code examples |

| SDK documentation | Code examples |
| --- | --- |
| AWS SDK for PHP | AWS SDK for PHP code examples |
| AWS Tools for PowerShell | AWS Tools for PowerShell code examples |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) code examples |
| AWS SDK for Ruby | AWS SDK for Ruby code examples |
| AWS SDK for Rust | AWS SDK for Rust code examples |
| AWS SDK for SAP ABAP | AWS SDK for SAP ABAP code examples |
| AWS SDK for Swift | AWS SDK for Swift code examples |

For examples specific to AWS Config, see Code examples for AWS Config using AWS SDKs.

**Example availability**

Can't find what you need? Request a code example by using the **Provide feedback** link at the bottom of this page.

# Working with the configuration recorder

The *configuration recorder* stores the configuration changes to the resource types in scope as configuration items (CIs).

There are two types of configuration recorders.

| Type | Description |
| --- | --- |
| Customer managed configuration recorder | A configuration recorder that you managed. The resource types in scope are set by you. By default, a customer managed configuration recorder records all supported resources in the AWS Region where AWS Config is running. |
| Service-linked configuration recorder | A configuration recorder that is linked to a specific AWS service. The resource types in scope are set by the linked service. |

**Topics**


- Considerations for the customer managed configuration recorder
- Considerations for service-linked configuration recorders
- Drift detection for the configuration recorder
- Starting the customer managed configuration recorder
- Stopping the customer managed configuration recorder
- Changing the recording frequency for the customer managed configuration recorder
- Renaming the customer managed configuration recorder
- Viewing your configuration recorders
- Deleting your configuration recorders

# Considerations for the customer managed configuration recorder

**One customer managed configuration recorder per account per Region**

You can have only one customer managed configuration recorder for each AWS account for each AWS Region.

**Default is to record all supported resource types, excluding the global IAM resource types**

The default for a customer managed configuration recorder is to record all supported resource types, excluding the following global IAM resource types: `AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User` You can specify which resource types you want to include or exclude from recording.

For more information, see Recording AWS Resources with AWS Config.

**You are charged service usage fees for using the customer managed configuration recorder**

You are charged service usage fees when AWS Config starts recording configurations with the customer managed configuration recorder.

For pricing information, see AWS Config Pricing.

**Use AWS Systems Manager to create a customer managed configuration recorder across an organization**

You can use AWS Systems Manager Quick Setup to create a customer managed configuration recorder across multiple organizational units (OUs) and AWS Regions using AWS best practices.

For more information, see Create an AWS Config configuration recorder using Quick Setup in the *Systems Manager User Guide*.

> **Important**
>
> **Policies and compliance results**
>
> IAM policies and other policies managed in AWS Organizations can impact whether AWS Config has permissions to record configuration changes for your resources. Additionally,

rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use AWS Config.

**Stale evaluation results for deleted resources can persist if the configuration recorder is turned off**

If the customer managed configuration recorder is turned off, it disables the ability of AWS Config Config to track changes to the configuration of the resources you specified, including their deletions. This means you might see stale evaluation results for resources that are deleted when the customer managed configuration recorder is turned off since AWS Config cannot capture deletion events if recording is not on.

## Considerations for service-linked configuration recorders

**The AWS Config service-linked role must be used**

The AWS Config service-linked role is required for service-linked configuration recorders.

For more information, see Using Service-Linked Roles for AWS Config.

**Service-linked configuration recorders are always recording**

Service-linked recorders are fixed. You can't directly change the settings in a service-linked recorder. To modify recorder settings such as starting, stopping, or updating the recorder, make these changes through the associated AWS service that uses the service-linked recorder.

For more information, see Deleting the Configuration Recorder.

**The recording scope determines if you receive configuration items**

The recording scope is set by the AWS service that is linked to the configuration recorder and determines whether you receive configuration items (CIs) in the delivery channel. If the recording scope is INTERNAL, you will not receive CIs in the delivery channel.

**The recording scope determines if you are charged a service fee**

The recording scope is set by the AWS service that is linked to the configuration recorder and determines whether the configuration items (CIs) in scope are recorded for free (INTERNAL) or if it impacts the costs of your bill (PAID).

### Recording frequency precedence between recorders

When you have both a customer managed configuration recorder and a service-linked configuration recorder with a recording scope of 'PAID' that record the same resource types, the recorder with the higher recording frequency takes precedence. For example, if your customer managed recorder is set to daily recording, but you enable an AWS service that uses a service-linked recorder with a recording scope of 'PAID' and continuous recording, the affected resource types will be recorded continuously.

This means that even though your customer managed recorder settings still show "Daily recording," you will be charged for continuous recording for the resource types that are in scope for both recorders. This only affects resource types that are being recorded by both recorders.

> **Note**
>
> You are charged only once per configuration item, regardless of the number of configuration items generated by a customer managed configuration recorder or service-linked configuration recorders that you pay for.

#### Example Example: Recording frequency precedence

You have configured your customer managed recorder to record Amazon EC2 instances with daily recording frequency. Later, you enable an AWS service feature that uses a service-linked recorder with a recording scope of 'PAID' and continuous recording that also records Amazon EC2 instances. In this scenario:

- Your customer managed recorder settings will still show "Daily recording"
- Amazon EC2 instances will be recorded continuously and provides additional CIs because the service-linked recorder with a recording scope of 'PAID' has a higher recording frequency
- You will be charged for continuous recording of Amazon EC2 instances
- Other resource types that are only recorded by your customer managed recorder will continue to be recorded in a daily recording frequency

## Supported services

Service-linked configuration recorders are supported for the following services:

| AWS service | Service principal | Benefits of using with AWS Config | Learn more |
| --- | --- | --- | --- |
| Amazon CloudWatch | `observabilityadmin.amazonaws.com`, `telemetry-enablement.observabilityadmin.amazonaws.com` | You can use Amazon CloudWatch Observability Admin to discover and understand the state of telemetry configuration in CloudWatch for your AWS Organization or account. | For more information, see Auditing CloudWatch telemetry configurations in the *CloudWatch User Guide*. |
| AWS Security Hub CSPM | `securityhub.amazonaws.com` | You can use AWS Security Hub CSPM to centrally manage security findings and perform security assessments across your AWS accounts. The service-linked recorder enables an event-driven approach for obtaining resource configuration items required for exposure analysis coverage. | For more information, see Enabling Security Hub in the *Security Hub CSPM User Guide*. |

## Drift detection for the configuration recorder

The `AWS::Config::ConfigurationRecorder` resource type is a *configuration item* (CI) for the configuration recorder that tracks all changes to the state of configuration recorder. You can use this CI to check if the state of the configuration recorder differs, or has *drifted*, from its previous state.

For example, this CI tracks if there are updates to resource types that you have enabled AWS Config to track, if you have stopped or started the configuration recorder, or if you have deleted or uninstalled the configuration recorder. A drifted configuration recorder indicates that you are not accurately detecting changes to your intended resource types. If your configuration recorder has been drifted, this can result in false negative or false positive compliance results.

The `AWS::Config::ConfigurationRecorder` resource type is a system resource type of AWS Config and recording of this resource type is enabled by default in all supported Regions. Recording for the `AWS::Config::ConfigurationRecorder` resource type comes with no additional charge.

## Starting the customer managed configuration recorder

You can use the AWS Config console or the AWS CLI start the customer managed configuration recorder.

To start the customer managed configuration recorder (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Start recording**. When prompted, choose **Confirm**.

To start the customer managed configuration recorder (CLI)

Use the `start-configuration-recorder` command:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

## Stopping the customer managed configuration recorder

> **Note**
>
> **Service-linked configuration recorders are always recording**

> You cannot stop a service-linked configuration recorder because service-linked configuration recorders are always recording. To stop recording, you must delete the service-linked configuration recorder. For more information, see Deleting the Configuration Recorder.

You can use the AWS Config console or the AWS CLI stop the customer managed configuration recorder.

To stop the customer managed configuration recorder (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Stop recording**. When prompted, choose **Confirm**.

To stop the customer managed configuration recorder (CLI)

Use the `stop-configuration-recorder` command:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

## Changing the recording frequency for the customer managed configuration recorder

AWS Config supports continuous recording and daily recording:

- *Continuous recording* allows you to record configuration changes continuously whenever a change occurs.
- *Daily recording* allows you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded. For more information see, Recording Frequency.

You can use the AWS Config console or the AWS CLI change the recording frequency.

To change the recording frequency for the customer managed configuration recorder (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Start recording**.
4. For **Recording method managed recorder**, choose **All resource types with customizable overrides**.
5. For **Default settings**, choose a recording frequency.
6. Choose **Save**.

To change the recording frequency (CLI)

Use the `put-configuration-recorder` command to change the recording frequency for the configuration recorder:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`). You can also use this field override the recording frequency for specific resource types.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

`put-configuration-recorder` uses the following fields for the `--configuration-recorder` parameter:

- `name` – The name of the configuration recorder. AWS Config automatically assigns the name of "default" when creating the configuration recorder.
- `roleARN` – Amazon Resource Name (ARN) of the IAM role assumed by AWS Config and used by the configuration recorder.
- `recordingMode` – Specifies the default recording frequency that AWS Config uses to record configuration changes. AWS Config supports *Continuous recording* and *Daily recording*. Continuous recording allows you to record configuration changes continuously whenever a change occurs. Daily recording allows you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.
  - `recordingFrequency` – The default recording frequency that AWS Config uses to record configuration changes.

    > **Note**
    >
    > AWS Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

  - `recordingModeOverrides` – This field allows you to specify your overrides for the recording mode. It is an array of `recordingModeOverride` objects. Each `recordingModeOverride` object in the `recordingModeOverrides` array consists of three fields:
    - `description` – A description that you provide for the override.
    - `recordingFrequency` – The recording frequency that will be applied to all the resource types specified in the override.
    - `resourceTypes` – A comma-separated list that specifies which resource types AWS Config includes in the override.

> **Note**
>
> **Required and optional fields**

The `recordingMode` field for `put-configuration-recorder` is optional. By default, the recording frequency for the configuration recorder is set to Continuous recording.

> **Note**
>
> **Limits**
>
> Daily recording is not supported for the following resource types:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> For the **Record all current and future supported resource types** (`ALL_SUPPORTED_RESOURCE_TYPES`) recording strategy, these resource types will be set to Continuous recording.

## Renaming the customer managed configuration recorder

You must use the AWS CLI to rename the customer managed configuration recorder. To change the name of the customer managed configuration recorder, you must delete it and create a new configuration recorder with your specified name.

**Renaming the customer managed configuration recorder using the AWS CLI**

1. Use the `describe-configuration-recorders` command to look up the name of your current customer managed configuration recorder:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. Use the `delete-configuration-recorder` command to delete your customer managed current configuration recorder:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. Use the `put-configuration-recorder` command to create a customer managed configuration recorder with the new name:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Use the `start-configuration-recorder` command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

## Viewing your configuration recorders

You can use the AWS Config console or the AWS CLI view details about your configuration recorders.

To view your configuration recorders (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the navigation pane.
3. For the customer managed configuration recorder, you can view details on the **Customer managed recorder** tab.
4. For service-linked configuration recorders, choose a service-linked configuration recorders on the **Service-linked recorders** tab, and then choose **View**.

To view your configuration recorders (CLI)

Use the `describe-configuration-recorders` command to view details about your configuration recorders:

```
$ aws configservice describe-configuration-recorders
```

```
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Use the `describe-configuration-recorder-status` command to view the current status of your configuration recorders:

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

For both of these commands, you can use the `arn` and `configuration-recorder-names` fields to specify a list of configuration recorders. For service-linked configuration recorders, you can use the `service-principal` field to specify a configuration recorder.

If a configuration recorder is not specified, this command returns the details of all configuration recorders associated with the account.

## Deleting your configuration recorders

You must use the AWS CLI to delete the customer managed configuration recorder. You can use AWS Config console or the AWS CLI to delete a service-linked configuration recorder.

To delete the customer managed configuration recorder (CLI)

Use the `delete-configuration-recorder` command:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To delete a service-linked configuration recorder (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Service-linked recorders** tab, choose a service-linked configuration recorders on the **Service-linked recorders** tab, and then choose **Delete**. When prompted, choose **Delete**.

To delete a service-linked configuration recorder (CLI)

Use the `delete-service-linked-configuration-recorder` command:

This command uses the `--service-principal` field.

```
$ aws configservice delete-service-linked-configuration-recorder --service-principal
 "The service principal of the AWS service for the service-linked configuration
 recorder that you want to delete"
```

# Working with the Delivery Channel

As AWS Config continually records the changes that occur to your AWS resources, it sends notifications and updated configuration states through the *delivery channel*. You can manage the delivery channel to control where AWS Config sends configuration updates.

**Topics**


- Considerations
- Terminology
- Components of a Configuration Item
- Viewing the Delivery Channel
- Updating the Delivery Channel
- Renaming the Delivery Channel
- Delivering Configuration Snapshots to an Amazon S3 Bucket
- Verifying Delivery Status
- Viewing Configuration Snapshots in Amazon S3 bucket
- Example Configuration Snapshot from AWS Config
- Notifications that AWS Config Sends to an Amazon SNS topic


## Considerations

**One delivery channel per Region per account**

You can have only one delivery channel per AWS Region region per AWS account, and the delivery channel is required to use AWS Config.

**Oversized configuration item notifications include a brief summary**

When AWS Config detects a configuration change for a resource and the notification exceeds the maximum size allowed by Amazon SNS, the notification includes a brief summary of the configuration item. You can view the complete notification in the Amazon S3 bucket location specified in the `s3BucketLocation` field. For more information, see Example Oversized Configuration Item Change Notification.

**AWS Config supports AWS KMS encryption for Amazon S3 buckets used by AWS Config**

You can provide an AWS Key Management Service (AWS KMS) key or alias Amazon Resource Name (ARN) to encrypt the data delivered to your Amazon Simple Storage Service (Amazon S3) bucket. By default, AWS Config delivers configuration history and snapshot files to your Amazon S3 bucket and encrypts the data at rest using S3 AES-256 server-side encryption, SSE-S3. However, if you provide AWS Config with your KMS key or alias ARN, AWS Config uses that KMS key instead of AES-256 encryption.

AWS Config does not support the delivery channel to an Amazon S3 bucket where object lock is enabled with default retention enabled. For more information, see How S3 Object Lock works.

# Terminology

A *configuration item* represents a point-in-time view of the various attributes of a supported AWS resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if AWS Config is recording Amazon S3 buckets, AWS Config creates a configuration item whenever a bucket is created, updated, or deleted. You can also select for AWS Config to create a configuration item at the recording frequency that you set.

A *configuration history* is a collection of the configuration items for a given resource over any time period. A configuration history can help you answer questions about, for example, when the resource was first created, how the resource has been configured over the last month, and what configuration changes were introduced yesterday at 9 AM. The configuration history is available to you in multiple formats. AWS Config automatically delivers a configuration history file for each resource type that is being recorded to an Amazon S3 bucket that you specify. You can select a given resource in the AWS Config console and navigate to all previous configuration items for that resource using the timeline. Additionally, you can access the historical configuration items for a resource from the API.

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally,

you can select a point in time in the AWS Config console and navigate through the snapshot of configuration items using the relationships between the resources.

A *configuration stream* is an automatically updated list of all configuration items for the resources that AWS Config is recording. Every time a resource is created, modified, or deleted, AWS Config creates a configuration item and adds to the configuration stream. The configuration stream works by using an Amazon Simple Notification Service (Amazon SNS) topic of your choice. The configuration stream is helpful for observing configuration changes as they occur so that you can spot potential problems, generating notifications if certain resources are changed, or updating external systems that need to reflect the configuration of your AWS resources.

## Components of a Configuration Item

A *configuration item* represents a point-in-time view of the various attributes of a supported AWS resource that exists in your account. The components of a configuration item include metadata, attributes, relationships, current configuration, and related events. AWS Config creates a configuration item whenever it detects a change to a resource type that it is recording. For example, if AWS Config is recording Amazon S3 buckets, AWS Config creates a configuration item whenever a bucket is created, updated, or deleted. You can also select for AWS Config to create a configuration item at the recording frequency that you set.

A configuration item consists of the following components.

| Component | Description | Contains |
| --- | --- | --- |
| Metadata | Information about this configuration item | • Version ID<br>• Time when the configuration item was captured<br>• Status of the configuration item indicatin g whether the item was captured successfully<br>• State ID indicating the ordering of the configuration items of a resource |
| Attributes | Resource attributes | • Resource ID<br>• List of key–value tags for this resource |

| Component | Description | Contains |
| --- | --- | --- |
| | | • Resource type (see Supported Resource Types for AWS Config)<br>• Amazon Resource Name (ARN)<br>• Availability Zone that contains this resource, if applicable<br>• Time the resource was created |
| Relationships | How the resource is related to other resources associated with the account | Description of the relationship, such as Amazon EBS volume `vol-1234567` is attached to an Amazon EC2 instance `i-a1b2c3d4` |
| Current configuration | Information returned through a call to the Describe or List API of the resource | For example, `DescribeVolumes` API returns the following information about the volume:<br>• Availability Zone the volume is in<br>• Time the volume was attached<br>• ID of the EC2 instance it is attached to<br>• Current status of the volume<br>• State of DeleteOnTermination flag<br>• Device the volume is attached to<br>• Type of volume, such as `gp2`, `io1`, or `standard` |

**Notes**

1. A configuration item relationship does not include network flow or data flow dependencies. Configuration items cannot be customized to represent your application architecture.
2. As of Version 1.3, the relatedEvents field is empty. You can access the LookupEvents API in the *AWS CloudTrail API Reference* to retrieve the events for the resource.
3. As of Version 1.3, the configurationItemMD5Hash field is empty. You can use the configurationStateId field to ensure you have the latest configuration item.

4. If a resource type does not support tagging or does not include tag information in its describe API response, AWS Config won't capture tag data in the configuration items (CIs) for that resource type. AWS Config will still record these resources. However, any functionality that relies on tag data won't work. This affects tag-based filtering, grouping, or compliance evaluation that relies on tag data.

# Viewing the Delivery Channel

You must use the AWS CLI to view details about the delivery channel.

The following code examples show how to use `DescribeDeliveryChannels`.

CLI

**AWS CLI**

**To get details about the delivery channel**

The following command returns details about the delivery channel:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- For API details, see DescribeDeliveryChannels in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example retrieves the delivery channel for the region and displays details.**

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

**Output:**

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example retrieves the delivery channel for the region and displays details.**

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

**Output:**

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

# Updating the Delivery Channel

When you update the delivery channel, you can set the following options:

- The Amazon S3 bucket where AWS Config sends configuration snapshots and configuration history files.
- How often AWS Config delivers configuration snapshots to your Amazon S3 bucket.
- The Amazon SNS topic to which AWS Config sends notifications about configuration changes.

## To update the delivery channel (Console)

You can use the AWS Config console to set the Amazon S3 bucket and the Amazon SNS topic for your delivery channel. For steps to manage these settings, see Setting Up AWS Config with the Console.

The console does not provide options to rename the delivery channel, set the frequency for configuration snapshots, or delete the delivery channel. To do these tasks, you must use the AWS CLI, the AWS Config API, or one of the AWS SDKs.

## To update the delivery channel (AWS SDKs)

The following code examples show how to use `PutDeliveryChannel`.

CLI

**AWS CLI**

**To create a delivery channel**

The following command provides the settings for the delivery channel as JSON code:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
```

```
}
```

This example sets the following attributes:

`name` - The name of the delivery channel. By default, AWS Config assigns the name `default` to a new delivery channel.You cannot update the delivery channel name with the `put-delivery-channel` command. For the steps to change the name, see Renaming the Delivery Channel.`s3BucketName` - The name of the Amazon S3 bucket to which AWS Config delivers configuration snapshots and configuration history files.If you specify a bucket that belongs to another AWS account, that bucket must have policies that grant access permissions to AWS Config. For more information, see Permissions for the Amazon S3 Bucket.

`snsTopicARN` - The Amazon Resource Name (ARN) of the Amazon SNS topic to which AWS Config sends notifications about configuration changes.If you choose a topic from another account, the topic must have policies that grant access permissions to AWS Config. For more information, see Permissions for the Amazon SNS Topic.

`configSnapshotDeliveryProperties` - Contains the `deliveryFrequency` attribute, which sets how often AWS Config delivers configuration snapshots and how often it invokes evaluations for periodic Config rules.

If the command succeeds, AWS Config returns no output. To verify the settings of your delivery channel, run the describe-delivery-channels command.

- For API details, see PutDeliveryChannel in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example changes the deliveryFrequency property of an existing delivery channel.**

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example changes the deliveryFrequency property of an existing delivery channel.**

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

(Optional) You can use the `describe-delivery-channels` command to verify that the delivery channel settings are updated:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

The following code examples show how to use `DescribeDeliveryChannels`.

CLI

**AWS CLI**

**To get details about the delivery channel**

The following command returns details about the delivery channel:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- For API details, see DescribeDeliveryChannels in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example retrieves the delivery channel for the region and displays details.**

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

**Output:**

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example retrieves the delivery channel for the region and displays details.**

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

**Output:**

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

# Renaming the Delivery Channel

To change the delivery channel name, you must delete it and create a new delivery channel with your specified name. Before you can delete the delivery channel, you must temporarily stop the configuration recorder. The AWS Config console does not provide the option to delete the delivery channel. You must use the AWS CLI, the AWS Config API, or one of the AWS SDKs.

### Renaming the delivery channel using the AWS CLI

1. Use the `stop-configuration-recorder` command to stop the configuration recorder:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. Use the `describe-delivery-channels` command, and take note of your delivery channel's attributes:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. Use the `delete-delivery-channel` command to delete the delivery channel:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Use the `put-delivery-channel` command to create a delivery channel with the desired name:

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

The deliveryChannel.json file specifies the delivery channel attributes:

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Use the `start-configuration-recorder` command to resume recording:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

# Delivering Configuration Snapshots to an Amazon S3 Bucket

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the AWS Config console and navigate through the snapshot of configuration items using the relationships between the resources.

## Delivering Configuration Snapshots

AWS Config generates configuration snapshots when you invoke the DeliverConfigSnapshot action or you run the AWS CLI `deliver-config-snapshot` command. AWS Config stores configuration snapshots in the Amazon S3 bucket that you specified when you enabled AWS Config.

Enter the `deliver-config-snapshot` command by specifying the name assigned by AWS Config when you configured your delivery channel, for example:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

## Verifying Delivery Status

Enter the `describe-delivery-channel-status` command to verify that the AWS Config has started delivering the configurations to the specified delivery channel:

```
aws configservice describe-delivery-channel-status
```

The response lists the status of all the three delivery formats that AWS Config uses to deliver configurations to your bucket and topic.

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
```

```
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

View the `lastSuccessfulTime` field in `configSnapshotDeliveryInfo`. The time should match the time you last requested the delivery of the configuration snapshot.

> **Note**
>
> AWS Config uses the UTC format (Coordinated Universal Time) to record the time.

# Viewing Configuration Snapshots in Amazon S3 bucket

A *configuration snapshot* is a collection of the configuration items for the supported resources that exist in your account. This configuration snapshot is a complete picture of the resources that are being recorded and their configurations. The configuration snapshot can be a useful tool for validating your configuration. For example, you may want to examine the configuration snapshot regularly for resources that are configured incorrectly or that potentially should not exist. The configuration snapshot is available in multiple formats. You can have the configuration snapshot delivered to an Amazon Simple Storage Service (Amazon S3) bucket that you specify. Additionally, you can select a point in time in the AWS Config console and navigate through the snapshot of configuration items using the relationships between the resources.

## Viewing Configuration Snapshots

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. In the Amazon S3 console **All Buckets** list, choose the name of your Amazon S3 bucket.
3. Go through the nested folders in your bucket until you see the `ConfigSnapshot` object with a snapshot ID that matches with the ID returned by the command. Download and open the object to view the configuration snapshot.. The S3 bucket also contains an empty file named `ConfigWritabilityCheckFile`. AWS Config creates this file to verify that the service can successfully write to the S3 bucket.

# Example Configuration Snapshot from AWS Config

The following is an example of the information that AWS Config includes in a configuration snapshot. The snapshot describes the configuration for the resources that AWS Config is recording in the current region for your AWS account, and it describes the relationships between these resources.

> **Note**
>
> The configuration snapshot can include references to resources types and resource IDs that are not supported.


```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
```

```
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
```

```
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
```

```
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
```

```
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
```

```
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

The next step is to verify that configuration snapshot was delivered successfully to the delivery channel.

## Notifications that AWS Config Sends to an Amazon SNS topic

> **Note**
>
> Before AWS Config can send notifications to an Amazon SNS topic, you must first set up the configuration recorder and the delivery channel. For more information, see Managing the Configuration Recorder and Managing the Delivery Channel.

You can configure AWS Config to stream configuration changes and notifications to an Amazon SNS topic. For example, when a resource is updated, you can get a notification sent to your email, so that you can view the changes. You can also be notified when AWS Config evaluates your custom or managed rules against your resources. For more information, see Logging and Monitoring in AWS Config.

AWS Config sends notifications for the following events:

- Configuration item change for a resource.
- Configuration history for a resource was delivered for your account.
- Configuration snapshot for recorded resources was started and delivered for your account.
- Compliance state of your resources and whether they are compliant with your rules.
- Evaluation started for a rule against your resources.

- AWS Config failed to deliver the notification to your account.

**Topics**


- Example Configuration Item Change Notifications
- Example Configuration History Delivery Notification
- Example Configuration Snapshot Delivery Started Notification
- Example Configuration Snapshot Delivery Notification
- Example Compliance Change Notification
- Example Rules Evaluation Started Notification
- Example Oversized Configuration Item Change Notification
- Example Delivery Failed Notification


## Example Configuration Item Change Notifications

AWS Config uses Amazon SNS to deliver notifications to subscription endpoints. These notifications provide the delivery status for configuration snapshots and configuration histories, and they provide each configuration item that AWS Config creates when the configurations of recorded AWS resources change. AWS Config also sends notifications that show whether your resources are compliant against your rules. If you choose to have notifications sent by email, you can use filters in your email client application based on the subject line and message body of the email.

The following is an example payload of an Amazon SNS notification that is generated when AWS Config detects that the Amazon Elastic Block Store volume `vol-ce676ccc` is attached to the instance with an ID of `i-344c463d`. The notification contains the configuration item change for the resource.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
```

```
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "awsAccountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
```

```
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```


## Configuration Items for Resources with Relationships

If a resource is related to other resources, a change to that resource can result in multiple configuration items. The following example shows how AWS Config creates configuration items for resources with relationships.

1. You have an Amazon EC2 instance with an ID of `i-007d374c8912e3e90`, and the instance is associated with an Amazon EC2 security group, `sg-c8b141b4`.
2. You update your EC2 instance to change the security group to another security group, `sg-3f1fef43`.

3. Because the EC2 instance is related to another resource, AWS Config creates multiple configuration items like the following examples:

This notification contains the configuration item change for the EC2 instance when the security group is replaced.


```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
```

```
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
```

```
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
```

```
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
                },
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
```

```
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
```

```
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
```

```
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
```

```
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

This notification contains the configuration item change for the EC2 security group, `sg-3f1fef43`, which is associated with the instance.

```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
```

```
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


## Understanding the `configurationItemDiff` field in Amazon SNS `ConfigurationItemChangeNotification` notifications

AWS Config creates a configuration item whenever the configuration of a resource changes (create/update/delete). For a list of supported resource types that AWS Config can record, see Supported Resource Types for AWS Config. AWS Config uses Amazon SNS to deliver a notification as the changes occur. The Amazon SNS notification payload includes fields to help you track the resource changes in a given AWS Region.

To understand why you receive a `ConfigurationItemChangeNotification` notification, review the `configurationItemDiff` details. The fields vary depending on the change type and can form different combinations such as UPDATE-UPDATE, UPDATE-CREATE, and DELETE-DELETE. The following are explanations of some common combinations.

**UPDATE-CREATE and UPDATE-UPDATE**

The following example includes changes in the resource direct relationships and resource configurations. The `configurationItemDiff` details reveal the following information:

**Action performed**: A managed policy present in the account was attached to an AWS Identity and Access Management (IAM) role.

**Basic operation performed**: UPDATE (updating the number of associations of the resource type `AWS::IAM::Policy` in an account).

**Change type combinations**:

1. Resource direct relationship change UPDATE-CREATE. A new attachment or association was created between an IAM policy and an IAM role.
2. Resource configuration change UPDATE-UPDATE. The number IAM policy associations increased from 2 to 3 when the policy was attached to the IAM role.

Example UPDATE-CREATE and UPDATE-UPDATE `configurationItemDiff` notification:

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
```

```
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

**UPDATE-DELETE**

The following example includes changes in the resource direct relationships and resource configurations. The `configurationItemDiff` details reveal the following information:

**Action performed**: A managed policy present in the account was detached from an IAM user.

**Basic operation performed**: UPDATE (updating the permissions policy associated with the resource type `AWS::IAM::User`).

**Change type combinations**: Resource direct relationship change UPDATE-DELETE. The association between an IAM user and an IAM policy in an account was deleted.

**DELETE-DELETE**

The following example includes changes in the resource direct relationships and resource configurations. The `configurationItemDiff` details reveal the following information:

**Action performed**: An IAM role present in an account was deleted.

**Basic operation performed**: DELETE (a resource of the resource type `AWS::IAM::Role` was deleted).

**Change type combinations**: Resource direct relationship change and resource configuration change DELETE-DELETE. The deletion of the IAM role also deleted the association of the IAM policy with the IAM role.

## Example Configuration History Delivery Notification

The configuration history is a collection of the configuration items for a resource type over a time period. The following is an example notification that AWS Config sends when the configuration history for a CloudTrail trail resource is delivered for your account.

```
{
```

```
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


## Example Configuration Snapshot Delivery Started Notification

The following is an example notification that AWS Config sends when AWS Config starts delivering the configuration snapshot for your account.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
```

```
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


## Example Configuration Snapshot Delivery Notification

The configuration snapshot is a collection of configuration items for all recorded resources and their configurations in your account. The following is an example notification that AWS Config sends when the configuration snapshot is delivered for your account.


```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
```

```
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## Example Compliance Change Notification

When AWS Config evaluates your resources against a custom or managed rule, AWS Config sends a notification that shows whether the resources are compliant against the rule.

The following is an example notification where the CloudTrail trail resource is compliant against the `cloudtrail-enabled` managed rule.

```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
```

```
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


### Example: Config Configuration Item Change | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
```

```
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
```

```
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

## Example Rules Evaluation Started Notification

AWS Config sends a notification when it starts to evaluate your custom or managed rule against your resources. The following is an example notification when AWS Config starts to evaluate the `iam-password-policy` managed rule.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
```

```
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

## Example Oversized Configuration Item Change Notification

When AWS Config detects a configuration change for a resource, it sends a configuration item (CI) notification. If the notification exceeds the maximum size allowed by Amazon Simple Notification Service (Amazon SNS), the notification includes a brief summary of the configuration item.

You can view the complete notification in the Amazon S3 bucket location specified in the `s3BucketLocation` field.

The following example notification shows a CI for an Amazon EC2 instance. The notification includes a summary of the changes and the location of the notification in the Amazon S3 bucket.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z
```

```
    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "amzn-s3-demo-bucket/AWSLogs/123456789012/
Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

## How to access oversized configuration items

When a configuration item is oversized, only a summary is sent to Amazon SNS. The complete configuration item (CI) is stored in Amazon S3

The following code example shows how to access the the complete CI.

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """

    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
 json.loads(value)
```

```
                print(f"Supplementary Configuration:
 {config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

### How it works

1. The function accepts an event parameter containing the AWS Config notification.
2. It checks if the message type is an oversized configuration notification.
3. The function extracts the resource type and ID from the summary.
4. Using the AWS Config client, it retrieves the complete configuration history.
5. The function processes both main and supplementary configurations.
6. If needed, you can access the complete notification from the provided S3 location.

## Example Delivery Failed Notification

AWS Config sends a delivery failed notification if AWS Config can't deliver the configuration snapshot or an oversized configuration item change notification to your Amazon S3 bucket. Verify that you specified a valid Amazon S3 bucket.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
```

```
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

# Viewing the AWS Config Dashboard

Use the **Dashboard** to see an overview of your resources, rules, conformance packs, and their compliance states and to visualize your AWS Config usage and success metrics with Amazon CloudWatch. This page helps you quickly identify the top resources in your AWS account, the conformance packs with the lowest level of compliance in your AWS account, what rules or resources are noncompliant in your AWS account, what traffic is driving your AWS Config usage, and key metrics for success and failure that have occured in your workflows.

**To use the AWS Config Dashboard**

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the left navigation pane, choose **Dashboard**.

**Contents**


- Compliance and Resource Inventory
- AWS Config Usage and Success Metrics


## Compliance and Resource Inventory

After setup, AWS Config starts recording your specified resources and evaluating them against your rules. It may take a few minutes for AWS Config to display your resources, rules, conformance packs, and their compliance states.

**Conformance packs by compliance score**

*Conformance packs by compliance score* displays up to 10 of your conformance packs with the lowest compliance score. A compliance score is the percentage of the number of compliant rule-resource combinations in a conformance pack compared to the number of total possible rule-resource combinations in the conformance pack.

This metric provides you with a high-level view of the compliance state of your conformance packs, and can be used to identify, investigate, and understand the level of compliance in your conformance packs. You can use the compliance score to track remediation progress, perform

comparisons across different sets of requirements, and see the impact a specific change or deployment has on a conformance pack.

To view the deployment status, compliance score, compliance score timeline, and rules for a conformance pack in a detailed view, choose the name of the conformance pack under **Conformance pack**.

**Compliance status**

*Compliance status* displays the number of your compliant and noncompliant rules and compliant and noncompliant resources. Resources are compliant or noncompliant based on an evaluation of the rule associated with it. If a resource does not follow the rule's specifications, the resource and the rule are flagged as noncompliant.

To view the list of noncompliant rules and resources, choose **Noncompliant rule(s)** or **Noncompliant resource(s)**.

**Rules by noncompliant resources**

*Rules by noncompliant resources* displays your top noncompliant rules in descending order by the number of resources. Choose a rule to view its details, parameters, and the resources in scope for that specific rule.

For a comprehensive list of noncompliant rules, choose **View all noncompliant rules**.

**Resource inventory**

*Resource inventory* displays the total number of resources that AWS Config is recording in descending order by the number of resources, and the count of each resource type in your AWS account. To open all resources for a resource type, choose that resource type to go to its **Resources inventory** page.

You can use the dropdown list to indicate which resource totals you want to view. By default, it is set to view **All resources**, but you can change it to AWS resources, Third-party resources, or Custom resources.

> **Note**
>
> The **Evaluate your AWS resource configuration using Config rules** message may appear on the **Dashboard** for the following reasons:

- You haven't set up AWS Config Rules for your AWS account. You can choose **Add rule** to go to the **Rules** page.
- AWS Config is still evaluating your resources against your rules. You can refresh the page to see the latest evaluation results.
- AWS Config evaluated your resources against your rules and did not find any resources in scope. You can specify the resources for AWS Config to record in the **Settings** page. For more information, see Recording AWS Resources with AWS Config.

## AWS Config Usage and Success Metrics

You can use Amazon CloudWatch dashboards in the AWS Config console to visualize your AWS Config usage and success metrics.

For each dashboard, you can do the following:

- Adjust the dashboard time range to display data from the past **3 Hours**, **1 Day**, or **1 Week**.
- Choose the **Calender icon**, to enter a custom time range: either a **Relative** time for a past specified amount of time or an **Absolute** time range between two dates.
- You can change the time format to display dashboard data in **UTC** (Coordinated Universal Time) or **Local time zone** (the time zone specified as your local time zone in the operating system of your device).
- Use the **Drop arrow** next the **Refresh icon** to specify how often the data in a dashboard should refresh, or to turn off the automatic refresh. Choose **Off**, **10 Seconds**, **1 Minute**, **2 Minutes**, **5 Minutes**, or **15 Minutes** to change the refresh internal.
- Choose **More options** (the vertical ellipsis menu) to add the AWS Config usage metrics or the AWS Config success metrics you are currently viewing in the AWS Config Dashboard to the CloudWatch console. This opens a new tab in the CloudWatch console that allows you to create a new custom dashboard in CloudWatch with information copied from your current AWS Config usage metrics or AWS Config success metrics.

If you want to perform additional analyses of these metrics with CloudWatch, choose **Metrics** in the left navigation pane of the CloudWatch console and then choose **AWS/Config**. For more information on what you can do from the CloudWatch console, see Using Amazon CloudWatch dashboards and Using Amazon CloudWatch metrics in the *CloudWatch User Guide*.

### AWS Config Usage Metrics

| Metric | Description | Unit | |
|---|---|---|---|
| `Configuration Items Recorded` | The number of configuration items recorded for each resource type or all resource types. A configuration item represents a point-in-time view of the various attributes of a supported AWS resource. For more information about configuration items or supported resource types, see Configuration Items and Supported Resource Types. | Count | |

You can select the resource type that you want to view by using the dropdown list. By default, it is set to view all resource types.

### AWS Config Success Metrics

| Metric | Description | Unit | |
|---|---|---|---|
| `Change Notifications Delivery Failed` | The number of failed change notification deliveries to the Amazon SNS topic for your delivery channel. A change notification informs you about a change to the configuration state of your AWS resources. You can use the ConfigStreamDeliveryInfo API to get the `lastErrorCode` or `lastErrorMessage` for the last attempted delivery for a change notification. For more information, see Managing the Delivery Channel. | Count | |
| `Config History Export Failed` | The number of failed configuration history exports to your Amazon S3 bucket. A configuration history is a collection of the configuration items for a given resource over a specified time period. For more | Count | |

| Metric | Description | Unit |
| --- | --- | --- |
| | information about configuration history, see Configuration History. | |
| `Configuration Recorder Insufficient Permissions Failure` | The number of failed permission access attempts due to the IAM role policy for all the configuration recorders in your account and AWS Region having insufficient permissions. The configuration recorder detects changes in to the resource types in scope. For the configuration recorder to record your AWS resource configurations, it requires the necessary IAM permissions. For more information, see IAM Role Policy for Getting Configuration Details. | Count |
| `Config Snapshot Export Failed` | The number of failed configuration snapshot exports to your Amazon S3 bucket. A configuration snapshot is a collection of the configuration items for the supported resources in your account. For more information about configuration snapshots, see Configuration Snapshot. | Count |

# Managing and Viewing AWS Resource Configurations with AWS Config

AWS Config allows you to assess, audit, and evaluate the configurations of AWS resources.

*AWS resources* are entities that you create and manage using the AWS Management Console, the AWS Command Line Interface (CLI), the AWS SDKs, or AWS partner tools. Examples of AWS resources include Amazon EC2 instances, security groups, Amazon VPCs, and Amazon Elastic Block Store. AWS Config refers to each resource using its unique identifier, such as the resource ID or an Amazon Resource Name (ARN).

Some common use cases include:

- **Cloud administrator**: You can track and manage resource configurations to help ensure compliance, troubleshoot issues, and maintain an understanding of your AWS environment
- **Security analyst**: You can evaluate resource configurations against desired states to help identify vulnerabilities and assess security posture.
- **Compliance officer**: You can continuously audit and monitor resource configurations to help ensure adherence to organizational policies and industry standards.

**Topics**


- Supported Resource Types for AWS Config
- Resource Coverage by Region Availability
- Recording AWS Resources with AWS Config
- Recording Configurations with AWS Config for Third-Party Resources using the AWS CLI
- Recording Software Configuration for Managed Instances with AWS Config
- Looking Up Resources That Are Discovered by AWS Config
- Viewing Compliance Information and Evaluation Results for your AWS Resources with AWS Config
- Viewing Compliance History for your AWS Resources with AWS Config
- Querying Compliance History for your AWS Resources
- Tagging Your AWS Config Resources

# Supported Resource Types for AWS Config

> **Important**
>
> This page is updated on a monthly cadence at the beginning of each month.

AWS Config supports the following AWS resources types and resource relationships.

- For more detailed information about a resource type, see its reference information (such as syntax, properties and return values) in the AWS resource and property types reference in the AWS CloudFormation User Guide.
- For AWS Config recording, some AWS Regions support a subset of these resource types. For information on which resource types are supported in which Regions, see Resource Coverage by Region Availability.
- Advanced queries for AWS Config supports a subset of these resource types. For a list of those supported resource types, see Supported Resource Types for Advanced Queries.
- Proactive evaluation for AWS Config supports a subset of these resource types. For a list of those supported resource types, see Supported Resource Types for Proactive Evaluation.
- Periodic rules run without the configuration recorder being enabled since periodic rules do not depend on configuration items (CIs). For more information on the difference between change–triggered rules and periodic rules, see Evaluation Mode and Trigger Types for AWS Config Rules.

  This means that if you view the rule page, there is no listed CI or supported resource. If you select the resource ID, you will see the following error: `The provided resource ID and resource type cannot be found`. This is expected behavior.

> **Note**
>
> **Region availability for resource types**
> Before specifying a resource type for AWS Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the AWS Region where you set up AWS Config. If a resource type is supported by AWS Config in at least one Region, you can enable the recording of that resource type in all Regions supported by AWS Config, even if the specified resource type is not supported in the AWS Region where you set up AWS Config.

**Tagging support for resource types**
If a resource type does not support tagging or does not include tag information in its describe API response, AWS Config won't capture tag data in the configuration items (CIs) for that resource type. AWS Config will still record these resources. However, any functionality that relies on tag data won't work. This affects tag-based filtering, grouping, or compliance evaluation that relies on tag data.

## Amazon AppStream

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon AppStream | `AWS::AppStream::Application` | NA | NA |
| | `AWS::AppStream::AppBlockBuilder` | NA | NA |
| | `AWS::AppStream::DirectoryConfig` | NA | NA |
| | `AWS::AppStream::Fleet` | NA | NA |
| | `AWS::AppStream::Stack` | NA | NA |

## Amazon AppFlow

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon AppFlow | `AWS::AppFlow::Flow` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon AppIntegrations | `AWS::AppIntegrations::EventIntegration` | NA | NA |
| | `AWS::AppIntegrations::Application` | NA | NA |

## Amazon API Gateway

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| API Gateway | `AWS::ApiGateway::Stage` | is contained in | ApiGateway Rest Api |
| | | is associated with | WAFRegional WebACL |
| | `AWS::ApiGateway::Method` | NA | NA Stage |
| | `AWS::ApiGateway::RestApi` | contains | ApiGateway Stage |
| | `AWS::ApiGateway::UsagePlan` | NA | NA |
| API Gateway V2 | `AWS::ApiGatewayV2::Stage` | is contained in | ApiGatewayV2 Api |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::ApiGatewayV2::Api` | contains | ApiGatewayV2 Stage |
| | `AWS::ApiGatewayV2::Integration` | NA | NA |

To learn more about how AWS Config integrates with Amazon API Gateway, see Monitoring API Gateway API Configuration with AWS Config.

## Amazon Athena

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Athena | `AWS::Athena::WorkGroup` | NA | NA |
| | `AWS::Athena::DataCatalog` | NA | NA |
| | `AWS::Athena::PreparedStatement` | NA | NA |

## Amazon Bedrock

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Bedrock | `AWS::Bedrock::ApplicationInferenceProfile` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::Bedrock::Guardrail` | NA | NA |
| | `AWS::Bedrock::KnowledgeBase` | NA | NA |
| | `AWS::Bedrock::Prompt` | NA | NA |

## Amazon Bedrock AgentCore

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Bedrock AgentCore | `AWS::BedrockAgentCore::BrowserCustom` | NA | NA |
| | `AWS::BedrockAgentCore::Runtime` | NA | NA |

## Amazon CloudFront

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon CloudFront | `AWS::CloudFront::Distribution` | is associated with | AWS WAF WebACL |
| | | | ACM Certificate |
| | | | S3 Bucket |
| | | | IAM Server Certificate |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::CloudFront::KeyValueStore` | NA | NA |
| | `AWS::CloudFront::PublicKey` | NA | NA |
| | `AWS::CloudFront::StreamingDistribution` | is associated with | AWS WAF WebACL |
| | | | ACM Certificate |
| | | | S3 Bucket |
| | | | IAM Server Certificate |
| | `AWS::CloudFront::RealtimeLogConfig` | NA | NA |

## Amazon CloudWatch

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon CloudWatch | `AWS::CloudWatch::Alarm` | NA | NA |
| | `AWS::CloudWatch::MetricStream` | NA | NA |
| Amazon CloudWatch Logs | `AWS::Logs::Destination` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon CloudWatch RUM | `AWS::RUM::AppMonitor` | NA | NA |
| Amazon CloudWatch Evidently | `AWS::Evidently::Project` | NA | NA |
| | `AWS::Evidently::Launch` | NA | NA |
| | `AWS::Evidently::Segment` | NA | NA |

## Amazon CodeGuru

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon CodeGuru Reviewer | `AWS::CodeGuruReviewer::RepositoryAssociation` | NA | NA |
| Amazon CodeGuru Profiler | `AWS::CodeGuruProfiler::ProfilingGroup` | NA | NA |

## Amazon Cognito

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Cognito | `AWS::Cognito::UserPool` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::Cognito::UserPoolClient` | NA | NA |
| | `AWS::Cognito::UserPoolGroup` | NA | NA |
| | `AWS::Cognito::IdentityPool` | NA | NA |

## Amazon Comprehend

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Comprehend | `AWS::Comprehend::Flywheel` | NA | NA |

## Amazon Connect

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Connect | `AWS::Connect::PhoneNumber` | NA | NA |
| | `AWS::Connect::QuickConnect` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::Connect::Instance` | NA | NA |
| | `AWS::Connect::Rule` | NA | NA |
| | `AWS::Connect::SecurityProfile` | NA | NA |
| | `AWS::Connect::User` | NA | NA |
| Amazon Connect Customer Profiles | `AWS::CustomerProfiles::Domain` | NA | NA |
| | `AWS::CustomerProfiles::ObjectType` | NA | NA |

## Amazon Detective

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Detective | `AWS::Detective::Graph` | NA | NA |

## Amazon DynamoDB

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon DynamoDB | `AWS::DynamoDB::Table` | NA | NA |

## Amazon Elastic Compute Cloud

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Elastic Compute Cloud | `AWS::EC2::Host` * | contains | EC2 instance |
| | `AWS::EC2::EIP` | is attached to | EC2 instance |
| | | | Network interface |
| | `AWS::EC2::Instance` | contains | EC2 network interface |
| | | is associated with | EC2 security group |
| | | is attached to | Amazon EBS volume |
| | | | EC2 Elastic IP (EIP) |
| | | is contained in | EC2 Dedicated host |
| | | | Route table |
| | | | Subnet |
| | | | Virtual private cloud (VPC) |
| | `AWS::EC2::NetworkInterface` | is associated with | EC2 security group |
| | | is attached to | EC2 Elastic IP (EIP) |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | | | EC2 instance |
| | | is contained in | Route table |
| | | | Subnet |
| | | | Virtual private cloud (VPC) |
| | `AWS::EC2::SecurityGroup` * | is associated with | EC2 instance |
| | | | EC2 network interface |
| | | | Virtual private cloud (VPC) |
| | `AWS::EC2::NatGateway` | is contained in | Virtual private cloud (VPC) |
| | | is contained in | Subnet |
| | `AWS::EC2::EgressOnlyInternetGateway` | is attached to | Virtual private cloud (VPC) |
| | `AWS::EC2::EC2Fleet` | NA | NA |
| | `AWS::EC2::SpotFleet` | NA | NA |
| | `AWS::EC2::SubnetNetworkAclAssociation` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::EC2::PrefixList` | NA | NA |
| | `AWS::EC2::FlowLog` | NA | NA |
| | `AWS::EC2::TransitGateway` | NA | NA |
| | `AWS::EC2::TransitGatewayAttachment` | NA | NA |
| | `AWS::EC2::TransitGatewayRouteTable` | NA | NA |
| | `AWS::EC2::VPCEndpoint` | is contained in | Virtual private cloud (VPC) |
| | | is attached to | Network interface |
| | | is contained in | Subnet |
| | | is contained in | Route table |
| | `AWS::EC2::VPCEndpointService` | is associated with | ElasticLoadBalancingV2 LoadBalancer |
| | `AWS::EC2::VPCPeeringConnection` | is associated with | Virtual private cloud (VPC) |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | AWS::EC2::RegisteredHAInstance | is associated with | EC2 instance |
| | AWS::EC2::SubnetRouteTableAssociation | NA | NA |
| | AWS::EC2::LaunchTemplate | NA | NA |
| | AWS::EC2::NetworkInsightsAccessScopeAnalysis | NA | NA |
| | AWS::EC2::TrafficMirrorTarget | NA | NA |
| | AWS::EC2::TrafficMirrorSession | NA | NA |
| | AWS::EC2::DHCPOptions | NA | NA |
| | AWS::EC2::IPAM | NA | NA |
| | AWS::EC2::IPAMResourceDiscovery | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::EC2::IPAMResourceDiscoveryAssociation` | NA | NA |
| | `AWS::EC2::NetworkInsightsPath` | NA | NA |
| | `AWS::EC2::TrafficMirrorFilter` | NA | NA |
| | `AWS::EC2::CapacityReservation` | NA | NA |
| | `AWS::EC2::ClientVpnEndpoint` | NA | NA |
| | `AWS::EC2::CustomerGateway` | is attached to | VPN connection |
| | `AWS::EC2::InternetGateway` | is attached to | Virtual private cloud (VPC) |
| | `AWS::EC2::NetworkAcl` | NA | NA |
| | `AWS::EC2::RouteTable` | contains | EC2 instance |
| | | | EC2 network interface |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | | | Subnet |
| | | | VPN gateway |
| | | is contained in | Virtual private cloud (VPC) |
| | `AWS::EC2::Subnet` | contains | EC2 instance |
| | | | EC2 network interface |
| | | is attached to | Network ACL |
| | | is contained in | Route table |
| | | | Virtual private cloud (VPC) |
| | `AWS::EC2::VPC` | contains | EC2 instance |
| | | | EC2 network interface |
| | | | Network ACL |
| | | | Route table |
| | | | Subnet |
| | | is associated with | Security group |
| | | is attached to | Internet gateway |
| | | | VPN gateway |
| | `AWS::EC2::VPNConnection` | is attached to | Customer gateway |
| | | | VPN gateway |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::EC2::VPNConnectionRoute` | NA | NA |
| | `AWS::EC2::VPNGateway` | is attached to | Virtual private cloud (VPC) |
| | | | VPN connection |
| | | is contained in | Route table |
| | `AWS::EC2::IPAMScope` | NA | NA |
| | `AWS::EC2::CarrierGateway` | NA | NA |
| | `AWS::EC2::TransitGatewayConnect` | NA | NA |
| | `AWS::EC2::IPAMPool` | NA | NA |
| | `AWS::EC2::TransitGatewayMulticastDomain` | NA | NA |
| | `AWS::EC2::NetworkInsightsAccessScope` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | AWS::EC2::NetworkInsightsAnalysis | NA | NA |
| | AWS::EC2::VPCBlockPublicAccessOptions | NA | NA |
| | AWS::EC2::VPCBlockPublicAccessExclusion | NA | NA |
| | AWS::EC2::EIPAssociation | NA | NA |
| | AWS::EC2::InstanceConnectEndpoint | NA | NA |
| | AWS::EC2::SnapshotBlockPublicAccess | NA | NA |
| | AWS::EC2::VPCEndpointConnectionNotification | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::EC2::SecurityGroupVpcAssociation` | NA | NA |
| | `AWS::EC2::VerifiedAccessInstance` | NA | NA |
| | `AWS::EC2::IPAMPoolCidr` | NA | NA |
| | `AWS::EC2::SubnetCidrBlock` | NA | NA |
| | `AWS::EC2::VPCGatewayAttachment` | NA | NA |
| Amazon Elastic Block Store | `AWS::EC2::Volume` | is attached to | EC2 instance |
| EC2 Image Builder | `AWS::ImageBuilder::ContainerRecipe` | NA | NA |
| | `AWS::ImageBuilder::DistributionConfiguration` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::ImageBuilder::ImagePipeline` | NA | NA |
| | `AWS::ImageBuilder::ImageRecipe` | NA | NA |
| | `AWS::ImageBuilder::InfrastructureConfiguration` | NA | NA |
| | `AWS::ImageBuilder::LifecyclePolicy` | NA | NA |

*AWS Config records the configuration details of Dedicated hosts and the instances that you launch on them. As a result, you can use AWS Config as a data source when you report compliance with your server-bound software licenses. For example, you can view the configuration history of an instance and determine which Amazon Machine Image (AMI) it is based on. Then, you can look up the configuration history of the host, which includes details such as the numbers of sockets and cores, to check that the host complies with the license requirements of the AMI. For more information, see Tracking Configuration Changes with AWS Config in the *Amazon EC2 User Guide*.

*The EC2 SecurityGroup Properties definition contains IP CIDR blocks, which are converted to IP ranges internally, and may return unexpected results when trying to find a specific IP range. For workarounds to search for specific IP ranges, see Limitations for Advanced Queries.

## Amazon Elastic Container Registry

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Elastic Container Registry | `AWS::ECR::ReplicationConfiguration` | NA | NA |
| | `AWS::ECR::Repository` | NA | NA |
| | `AWS::ECR::RepositoryCreationTemplate` | NA | NA |
| | `AWS::ECR::RegistryPolicy` | NA | NA |
| | `AWS::ECR::PullThroughCacheRule` | NA | NA |
| Amazon Elastic Container Registry Public | `AWS::ECR::PublicRepository` | NA | NA |

## Amazon Elastic Container Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Elastic Container Service | `AWS::ECS::Cluster` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::ECS::TaskDefinition` | NA | NA |
| | `AWS::ECS::Service` * | NA | NA |
| | `AWS::ECS::TaskSet` | NA | NA |
| | `AWS::ECS::CapacityProvider` | NA | NA |

*This service currently only support the new Amazon Resource Name (ARN) format. For more information, see Amazon Resource Names (ARNs) and IDs in the ECS developer guide.

Old (not supported): `arn:aws:ecs:`*`region`*`:`*`aws_account_id`*`:service/`*`service-name`*

New (supported): `arn:aws:ecs:`*`region`*`:`*`aws_account_id`*`:service/`*`cluster-name`*`/`*`service-name`*

## Amazon Elastic File System

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Elastic File System | `AWS::EFS::FileSystem` | NA | NA |
| | `AWS::EFS::AccessPoint` | NA | NA |

## Amazon Elastic Kubernetes Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Elastic Kubernetes Service | `AWS::EKS::Cluster` | NA | NA |
| | `AWS::EKS::FargateProfile` | NA | NA |
| | `AWS::EKS::IdentityProviderConfig` | NA | NA |
| | `AWS::EKS::Addon` | NA | NA |

## Amazon EMR

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon EMR | `AWS::EMR::Studio` | NA | NA |
| | `AWS::EMR::SecurityConfiguration` | NA | NA |
| Amazon EMR Containers | `AWS::EMRContainers::VirtualCluster` | NA | NA |

## Amazon EMR Serverless

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon EMR Serverless | `AWS::EMRServerless::Application` | NA | NA |

## Amazon EventBridge

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon EventBridge | `AWS::Events::EventBus` | NA | NA |
| | `AWS::Events::ApiDestination` | NA | NA |
| | `AWS::Events::Archive` | NA | NA |
| | `AWS::Events::Endpoint` | NA | NA |
| | `AWS::Events::Connection` | NA | NA |
| | `AWS::Events::Rule` | NA | NA |
| Amazon EventBridge schemas | `AWS::EventSchemas::RegistryPolicy` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::EventSchemas::Discoverer` | NA | NA |
| | `AWS::EventSchemas::Schema` | NA | NA |
| | `AWS::EventSchemas::Registry` | NA | NA |

## Amazon Forecast

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Forecast | `AWS::Forecast::Dataset` | NA | NA |
| | `AWS::Forecast::DatasetGroup` | NA | NA |

## Amazon Fraud Detector

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Fraud Detector | `AWS::FraudDetector::Label` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::FraudDetector::EntityType` | NA | NA |
| | `AWS::FraudDetector::Variable` | NA | NA |
| | `AWS::FraudDetector::Outcome` | NA | NA |

## Amazon GameLift

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon GameLift | `AWS::GameLift::Build` | NA | NA |

## Amazon GuardDuty

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon GuardDuty | `AWS::GuardDuty::Detector` | NA | NA |
| | `AWS::GuardDuty::Filter` | NA | NA |
| | `AWS::GuardDuty::IPSet` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::GuardDuty::MalwareProtectionPlan` | NA | NA |
| | `AWS::GuardDuty::ThreatIntelSet` | NA | NA |

## Amazon Inspector

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Inspector | `AWS::InspectorV2::Filter` | NA | NA |
| | `AWS::InspectorV2::Activation` | NA | NA |

## Amazon Interactive Video Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Interactive Video Service | `AWS::IVS::Channel` | NA | NA |
| | `AWS::IVS::RecordingConfiguration` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | `AWS::IVS::Playback KeyPair` | NA | NA |

## Amazon Keyspaces (for Apache Cassandra)

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Keyspaces (for Apache Cassandra) | `AWS::Cassandra::Keyspace` | NA | NA |

## Amazon Location Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Location Service | `AWS::Location::APIKey` | NA | NA |

## Amazon OpenSearch Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon OpenSearch Service (legacy Elasticsearch) | `AWS::Elasticsearch::Domain` | is associated with | KMS Key |
| | | | EC2 security group |
| | | | EC2 subnet |
| | | | Virtual private cloud (VPC) |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon OpenSearch Service | `AWS::OpenSearch::Domain` | NA | NA |
| Amazon OpenSearch Serverless | `AWS::OpenSearchServerless::VpcEndpoint` | NA | NA |
| | `AWS::OpenSearchServerless::Collection` | NA | NA |
| | `AWS::OpenSearchServerless::SecurityConfig` | NA | NA |

**Amazon OpenSearch Service rename**

On September 8, 2021, Amazon Elasticsearch Service was renamed to Amazon OpenSearch Service. OpenSearch Service supports OpenSearch as well as legacy Elasticsearch OSS. For more information, see Amazon OpenSearch Service - Summary of changes.
You might continue to see your data for `AWS::OpenSearch::Domain` under the existing `AWS::Elasticsearch::Domain` resource type for several weeks, even if you upgrade one or more domains to OpenSearch.

## Amazon Personalize

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Personalize | `AWS::Personalize::Dataset` | NA | NA |
| | `AWS::Personalize::Schema` | NA | NA |
| | `AWS::Personalize::Solution` | NA | NA |
| | `AWS::Personalize::DatasetGroup` | NA | NA |

## Amazon Pinpoint

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Pinpoint | `AWS::Pinpoint::ApplicationSettings` | NA | NA |
| | `AWS::Pinpoint::Segment` | NA | NA |
| | `AWS::Pinpoint::App` | NA | NA |
| | `AWS::Pinpoint::Campaign` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::Pinpoint::InAppTemplate` | NA | NA |
| | `AWS::Pinpoint::EmailChannel` | NA | NA |
| | `AWS::Pinpoint::EmailTemplate` | NA | NA |
| | `AWS::Pinpoint::EventStream` | NA | NA |

## Amazon Quantum Ledger Database (Amazon QLDB)

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon QLDB | `AWS::QLDB::Ledger` | NA | NA |

## Amazon Kendra

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Kendra | `AWS::Kendra::Index` | NA | NA |

## Amazon Kinesis

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Kinesis | `AWS::Kinesis::Stream` | NA | NA |
| | `AWS::Kinesis::StreamConsumer` | NA | NA |
| Amazon Kinesis Analytics V2 | `AWS::KinesisAnalyticsV2::Application` | NA | NA |
| Amazon Data Firehose | `AWS::KinesisFirehose::DeliveryStream` | NA | NA |
| Kinesis video stream | `AWS::KinesisVideo::SignalingChannel` | NA | NA |
| | `AWS::KinesisVideo::Stream` | NA | NA |

## Amazon Lex

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Lex | `AWS::Lex::BotAlias` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | `AWS::Lex::Bot` | NA | NA |

## Amazon Lightsail

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Lightsail | `AWS::Lightsail::Disk` | NA | NA |
| | `AWS::Lightsail::Certificate` | NA | NA |
| | `AWS::Lightsail::Bucket` | NA | NA |
| | `AWS::Lightsail::StaticIp` | NA | NA |

## Amazon Lookout for Metrics

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Lookout for Metrics | `AWS::LookoutMetrics::Alert` | NA | NA |

## Amazon Lookout for Vision

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Lookout for Vision | `AWS::LookoutVision::Project` | NA | NA |

## Amazon Macie

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Macie | `AWS::Macie::Session` | NA | NA |

## Amazon Managed Grafana

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Managed Grafana | `AWS::Grafana::Workspace` | NA | NA |

## Amazon Managed Service for Prometheus

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Managed Service for Prometheus | `AWS::APS::RuleGroupsNamespace` | NA | NA |

## Amazon MemoryDB

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon MemoryDB | `AWS::MemoryDB::SubnetGroup` | NA | NA |

## Amazon MQ

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon MQ | `AWS::AmazonMQ::Broker` | NA | NA |

## Amazon Managed Streaming for Apache Kafka

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Managed Streaming for Apache Kafka | `AWS::MSK::Cluster` | NA | NA |
| | `AWS::MSK::Configuration` | NA | NA |
| | `AWS::MSK::BatchScramSecret` | NA | NA |
| | `AWS::MSK::ClusterPolicy` | NA | NA |
| | `AWS::MSK::ServerlessCluster` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | `AWS::MSK::VpcConnection` | NA | NA |
| Amazon Managed Streaming for Apache Kafka Connect | `AWS::KafkaConnect::Connector` | NA | NA |
| | `AWS::KafkaConnect::CustomPlugin` | NA | NA |

## Amazon Quick Suite

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Quick Suite | `AWS::QuickSight::DataSource` | NA | NA |
| | `AWS::QuickSight::Template` | NA | NA |
| | `AWS::QuickSight::Theme` | NA | NA |

## Amazon Redshift

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon Redshift | `AWS::Redshift::Cluster` | is associated with | Cluster parameter group |
| | | | Cluster security group |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | | | Cluster subnet group |
| | | | Security group |
| | | | Virtual private cloud (VPC) |
| | `AWS::Redshift::ClusterParameterGroup` | NA | NA |
| | `AWS::Redshift::ClusterSecurityGroup` | NA | NA |
| | `AWS::Redshift::ScheduledAction` | NA | NA |
| | `AWS::Redshift::ClusterSnapshot` | is associated with | Cluster |
| | | | Virtual private cloud (VPC) |
| | `AWS::Redshift::ClusterSubnetGroup` | is associated with | Subnet |
| | | | Virtual private cloud (VPC) |
| | `AWS::Redshift::EventSubscription` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::Redshift::EndpointAccess` | NA | NA |
| | `AWS::Redshift::EndpointAuthorization` | NA | NA |
| | `AWS::Redshift::Integration` | NA | NA |

## Amazon Relational Database Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Relational Database Service | `AWS::RDS::DBCluster` | contains | RDS DB instance |
| | | is associated with | RDS DB subnet group |
| | | | EC2 security group |
| | `AWS::RDS::DBClusterSnapshot` | is associated with | RDS DB cluster |
| | | | Virtual private cloud (VPC) |
| | `AWS::RDS::DBInstance` | is associated with | EC2 security group |
| | | | RDS DB security group |
| | | | RDS DB subnet group |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::RDS::DBSecurityGroup` | is associated with | EC2 security group |
| | | | Virtual private cloud (VPC) |
| | `AWS::RDS::DBSnapshot` | is associated with | Virtual private cloud (VPC) |
| | `AWS::RDS::DBSubnetGroup` | is associated with | EC2 security group |
| | | | Virtual private cloud (VPC) |
| | `AWS::RDS::EventSubscription` | NA | NA |
| | `AWS::RDS::GlobalCluster` | NA | NA |
| | `AWS::RDS::Integration` | NA | NA |
| | `AWS::RDS::OptionGroup` | NA | NA |

## Amazon Route 53

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Route 53 | `AWS::Route53::DNSSEC` | NA | NA |
| | `AWS::Route53::HostedZone` | NA | NA |
| | `AWS::Route53::HealthCheck` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Route 53 Profiles | AWS::Route53Profiles::Profile | NA | NA |
| | AWS::Route53Profiles::ProfileAssociation | NA | NA |
| Amazon Route 53 Resolver | AWS::Route53Resolver::ResolverEndpoint | NA | NA |
| | AWS::Route53Resolver::ResolverRule | NA | NA |
| | AWS::Route53Resolver::ResolverRuleAssociation | NA | NA |
| | AWS::Route53Resolver::FirewallDomainList | NA | NA |
| | AWS::Route53Resolver::FirewallRuleGroupAssociation | NA | NA |
| | AWS::Route53Resolver::ResolverQueryLoggingConfig | NA | NA |
| | AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | NA | NA |
| | AWS::Route53Resolver::FirewallRuleGroup | NA | NA |
| Amazon Application Recovery Controller (ARC) | AWS::Route53RecoveryReadiness::Cell | NA | NA |
| | AWS::Route53RecoveryReadiness::ReadinessCheck | NA | NA |
| | AWS::Route53RecoveryReadiness::RecoveryGroup | NA | NA |
| | AWS::Route53RecoveryControl::Cluster | NA | NA |
| | AWS::Route53RecoveryControl::ControlPanel | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | AWS::Route53RecoveryControl::RoutingControl | NA | NA |
| | AWS::Route53RecoveryControl::SafetyRule | NA | NA |
| | AWS::Route53RecoveryReadiness::ResourceSet | NA | NA |

## Amazon SageMaker AI

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon SageMaker AI | AWS::SageMaker::AppImageConfig | NA | NA |
| | AWS::SageMaker::CodeRepository | NA | NA |
| | AWS::SageMaker::DataQualityJobDefinition | NA | NA |
| | AWS::SageMaker::Domain | NA | NA |
| | AWS::SageMaker::EndpointConfig | NA | NA |
| | AWS::SageMaker::FeatureGroup | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | AWS::SageMaker::Image | NA | NA |
| | AWS::SageMaker::InferenceExperiment | NA | NA |
| | AWS::SageMaker::MlflowTrackingServer | NA | NA |
| | AWS::SageMaker::Model | NA | NA |
| | AWS::SageMaker::ModelBiasJobDefinition | NA | NA |
| | AWS::SageMaker::ModelExplainabilityJobDefinition | NA | NA |
| | AWS::SageMaker::ModelQualityJobDefinition | NA | NA |
| | AWS::SageMaker::NotebookInstance | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::SageMaker::NotebookInstanceLifecycleConfig` | NA | NA |
| | `AWS::SageMaker::StudioLifecycleConfig` | NA | NA |
| | `AWS::SageMaker::UserProfile` | NA | NA |
| | `AWS::SageMaker::Workteam` | NA | NA |

## Amazon Simple Email Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Simple Email Service | `AWS::SES::ConfigurationSet` | NA | NA |
| | `AWS::SES::ContactList` | NA | NA |
| | `AWS::SES::DedicatedIpPool` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::SES::MailManagerTrafficPolicy` | NA | NA |
| | `AWS::SES::Template` | NA | NA |
| | `AWS::SES::ReceiptFilter` | NA | NA |
| | `AWS::SES::ReceiptRuleSet` | NA | NA |

## Amazon Simple Notification Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Simple Notification Service | `AWS::SNS::Topic` | NA | NA |

## Amazon Simple Queue Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Simple Queue Service | `AWS::SQS::Queue` | NA | NA |

# Amazon Simple Storage Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Amazon Simple Storage Service | `AWS::S3::Bucket` * | NA | NA |
| | `AWS::S3::AccountPublicAccessBlock` | NA | NA |
| | `AWS::S3::MultiRegionAccessPoint` | NA | NA |
| | `AWS::S3::StorageLens` | NA | NA |
| | `AWS::S3::AccessGrant` | NA | NA |
| | `AWS::S3::AccessGrantsInstance` | NA | NA |
| | `AWS::S3::AccessGrantsLocation` | NA | NA |
| | `AWS::S3::AccessPoint` | NA | NA |
| | `AWS::S3::StorageLensGroup` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::S3Tables::TableBucket` | NA | NA |
| | `AWS::S3Tables::TableBucketPolicy` | NA | NA |
| Amazon S3 Express One Zone | `AWS::S3Express::DirectoryBucket` | NA | NA |
| | `AWS::S3Express::BucketPolicy` | NA | NA |

*If you configured AWS Config to record your S3 buckets, and are not receiving configuration change notifications, check that your S3 bucket policies have the required permissions. For more information, see Managing Permissions for S3 Bucket Recording.

**Amazon S3 Bucket Attributes**

AWS Config also records the following attributes for the Amazon S3 bucket resource type.

| Attributes | Description |
|---|---|
| AccelerateConfiguration | Transfer acceleration for data over long distances between your client and a bucket. |
| BucketAcl | Access control list used to manage access to buckets and objects. |
| BucketPolicy | Policy that defines the permissions to the bucket. |
| CrossOriginConfiguration | Allow cross-origin requests to the bucket. |

| Attributes | Description |
| --- | --- |
| LifecycleConfiguration | Rules that define the lifecycle for objects in your bucket. |
| LoggingConfiguration | Logging used to track requests for access to the bucket. |
| NotificationConfiguration | Event notifications used to send alerts or trigger workflows for specified bucket events. |
| ReplicationConfiguration | Automatic, asynchronous copying of objects across buckets in different AWS Regions. |
| RequestPaymentConfiguration | Requester pays is enabled. |
| TaggingConfiguration | Tags added to the bucket to categorize. You can also use tagging to track billing. |
| WebsiteConfiguration | Static website hosting is enabled for the bucket. |
| VersioningConfiguration | Versioning is enabled for objects in the bucket. |

For more information about the attributes, see Bucket Configuration Options in the *Amazon Simple Storage Service User Guide*.

## Amazon WorkSpaces

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| Amazon WorkSpaces | `AWS::WorkSpaces::ConnectionAlias` | NA | NA |
| | `AWS::WorkSpaces::Workspace` | NA | NA |

## AWS Amplify

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Amplify | `AWS::Amplify::App` | NA | NA |
| | `AWS::Amplify::Branch` | NA | NA |

## AWS AppConfig

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS AppConfig | `AWS::AppConfig::Application` | NA | NA |
| | `AWS::AppConfig::Environment` | NA | NA |
| | `AWS::AppConfig::ConfigurationProfile` | NA | NA |
| | `AWS::AppConfig::DeploymentStrategy` | NA | NA |
| | `AWS::AppConfig::HostedConfi` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `gurationVersion` | | |
| | `AWS::AppConfig::Extension` | NA | NA |
| | `AWS::AppConfig::ExtensionAssociation` | NA | NA |

## AWS App Runner

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS App Runner | `AWS::AppRunner::VpcConnector` | NA | NA |
| | `AWS::AppRunner::Service` | NA | NA |

## AWS App Mesh

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS App Mesh | `AWS::AppMesh::VirtualNode` | NA | NA |
| | `AWS::AppMesh::VirtualService` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::AppMesh::VirtualGateway` | NA | NA |
| | `AWS::AppMesh::VirtualRouter` | NA | NA |
| | `AWS::AppMesh::Route` | NA | NA |
| | `AWS::AppMesh::GatewayRoute` | NA | NA |
| | `AWS::AppMesh::Mesh` | NA | NA |

## AWS AppSync

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS AppSync | `AWS::AppSync::GraphQLApi` | NA | NA |

## AWS Audit Manager

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Audit Manager | `AWS::AuditManager::Assessment` | NA | NA |

## AWS Auto Scaling

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Auto Scaling | `AWS::AutoScaling::AutoScalingGroup` | contains | Amazon EC2 instance |
| | | is associated with | Classic Load Balancer |
| | | | Auto Scaling launch configuration |
| | | | Subnet |
| | `AWS::AutoScaling::LaunchConfiguration` | is associated with | Amazon EC2 security group |
| | `AWS::AutoScaling::ScalingPolicy` | is associated with | Auto Scaling group |
| | | | Alarm |
| | `AWS::AutoScaling::ScheduledAction` | is associated with | Auto Scaling group |
| | `AWS::AutoScaling::WarmPool` | NA | NA |

## AWS B2B Data Interchange

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS B2B Data Interchange | `AWS::B2BI::Capability` | NA | NA |

## AWS Backup

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Backup | `AWS::Backup::BackupPlan` | NA | NA* |
| | `AWS::Backup::BackupSelection` | NA | NA |
| | `AWS::Backup::BackupVault` | NA | NA* |
| | `AWS::Backup::RecoveryPoint` | NA | NA |
| | `AWS::Backup::ReportPlan` | NA | NA |
| | `AWS::Backup::RestoreTestingPlan` | Na | NA |
| AWS Backup Gateway | `AWS::BackupGateway::Hypervisor` | NA | NA |

Due to how AWS Backup works, some of these resource types relate to the other AWS Backup resource types in this table.

`AWS::Backup::BackupPlan` is related to `AWS::Backup::BackupSelection` where a Backup Plan has many selections, and `AWS::Backup::BackupVault` is related to `AWS::Backup::RecoveryPoint` where an AWS Backup Vault has multiple recovery points.

For more information, see Managing backups using backup plans and Working with backup vaults.

## AWS Batch

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Batch | `AWS::Batch::JobQueue` | NA | NA |
| | `AWS::Batch::ComputeEnvironment` | NA | NA |
| | `AWS::Batch::SchedulingPolicy` | NA | NA |

## AWS Billing and Cost Management

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Billing and Cost Management | `AWS::BCMDataExports::Export` | NA | NA |

## AWS Budgets

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Budgets | `AWS::Budgets::BudgetsAction` | NA | NA |

## AWS Certificate Manager

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Certificate Manager | `AWS::ACM::Certificate` | NA | NA |

## AWS Clean Rooms

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Clean Rooms ML | `AWS::CleanRoomsML::TrainingDataset` | NA | NA |

## AWS CloudFormation

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| CloudFormation | `AWS::CloudFormation::GuardHook` | NA | NA |
| | `AWS::CloudFormation::LambdaHook` | NA | NA |
| | `AWS::CloudFormation::Stack` * | contains | Supported AWS resource types |
| | `AWS::CloudFormation::StackSet` | NA | NA |

*AWS Config records configuration changes to CloudFormation stacks and supported resource types in the stacks. AWS Config does not record configuration changes for resource types in the stack that are not yet supported. Unsupported resource types appear in the supplementary configuration section of the configuration item for the stack.

## AWS CloudTrail

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS CloudTrail | `AWS::CloudTrail::Trail` | NA | NA |
| | `AWS::CloudTrail::EventDataStore` | NA | NA |

## AWS Cloud9

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Cloud9 | `AWS::Cloud9::EnvironmentEC2` | NA | NA |

**AWS Cloud9 access no longer available to new users**

After careful consideration, we have made the decision to close new customer access to AWS Cloud9, effective July 25, 2024. AWS Cloud9 existing customers can continue to use the service as normal. AWS continues to invest in security, availability, and performance improvements for AWS Cloud9, but we do not plan to introduce new features. For more information, see How to migrate from AWS Cloud9 to AWS IDE Toolkits or AWS CloudShell.

## AWS Cloud Map

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Service Discovery | `AWS::ServiceDiscovery::Service` | NA | NA |
| | `AWS::ServiceDiscovery::PublicDnsNamespace` | NA | NA |
| | `AWS::ServiceDiscovery::HttpNamespace` | NA | NA |
| `AWS::ServiceDiscovery::Instance` | NA | NA | |

## AWS CodeArtifact

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS CodeArtifact | `AWS::CodeArtifact::Repository` | NA | NA |
| | `AWS::CodeArtifact::Domain` | NA | NA |

## AWS CodeBuild

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS CodeBuild | `AWS::CodeBuild::Project` * | is associated with | S3 bucket |
| | | | IAM role |
| | `AWS::CodeBuild::ReportGroup` | NA | NA |

*To learn more about how AWS Config integrates with AWS CodeBuild, see Use AWS Config with AWS CodeBuild Sample.

## AWS CodeDeploy

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS CodeDeploy | `AWS::CodeDeploy::Application` | contains | DeploymentGroup |
| | `AWS::CodeDeploy::DeploymentConfig` | NA | NA |
| | `AWS::CodeDeploy::DeploymentGroup` | is contained in | Application |

## AWS CodePipeline

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS CodePipeline | `AWS::CodePipeline::Pipeline` * | is attached to | S3 bucket |
| | | is associated with | IAM role |
| | | | Code project |
| | | | Lambda function |
| | | | Cloudformation stack |
| | | | ElasticBeanstalk application |

*AWS Config records configuration changes to CodePipeline pipelines and supported resource types in the pipelines. AWS Config does not record configuration changes for resource types in the pipelines that are not yet supported. Unsupported resource types such as `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, and `ECS service` appear in the supplementary configuration section of the configuration item for the stack.

## AWS Config

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Config | `AWS::Config::AggregationAuthorization` | NA | NA |
| | `AWS::Config::ResourceCompliance` * | is associated with | All resources* |
| | `AWS::Config::Confo` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | rmancePackCompliance | | |
| | AWS::Config::ConfigurationRecorder * | NA | NA |
| | AWS::Config::ConformancePack | NA | NA |
| | AWS::Config::StoredQuery | NA | NA |

*The relationship between `AWS::Config::ResourceCompliance` and a related resource depends on how `AWS::Config::ResourceCompliance` reports compliance for that specific resource type.

*`AWS::Config::ConfigurationRecorder` is a system resource type of AWS Config and recording of this resource type is enabled by default.

> **Note**
>
> Recording for the `AWS::Config::ConformancePackCompliance` and `AWS::Config::ConfigurationRecorder` resource types come with no additional charge.

## AWS Database Migration Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Database Migration Service | `AWS::DMS::EventSubscription` | NA | NA |
| | `AWS::DMS::ReplicationSubnetGroup` | NA | NA |
| | `AWS::DMS::ReplicationInstance` | NA | NA |
| | `AWS::DMS::ReplicationTask` | NA | NA |
| | `AWS::DMS::Certificate` | NA | NA |
| | `AWS::DMS::Endpoint` | NA | NA |

## AWS DataSync

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS DataSync | `AWS::DataSync::Agent` | NA | NA |
| | `AWS::DataSync::LocationSMB` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | AWS::DataSync::LocationFSxLustre | NA | NA |
| | AWS::DataSync::LocationFSxWindows | NA | NA |
| | AWS::DataSync::LocationS3 | NA | NA |
| | AWS::DataSync::LocationEFS | NA | NA |
| | AWS::DataSync::LocationNFS | NA | NA |
| | AWS::DataSync::LocationHDFS | NA | NA |
| | AWS::DataSync::LocationObjectStorage | NA | NA |
| | AWS::DataSync::Task | NA | NA |

## AWS Deadline Cloud

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Deadline Cloud | `AWS::Deadline::Fleet` | NA | NA |
| | `AWS::Deadline::Monitor` | NA | NA |
| | `AWS::Deadline::QueueFleetAssociation` | NA | NA |

## AWS Device Farm

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Device Farm | `AWS::DeviceFarm::TestGridProject` | NA | NA |
| | `AWS::DeviceFarm::InstanceProfile` | NA | NA |
| | `AWS::DeviceFarm::Project` | NA | NA |

## AWS Elastic Beanstalk

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Elastic Beanstalk | `AWS::ElasticBeanstalk::Application` | contains | Elastic Beanstalk Application Version |
| | | | Elastic Beanstalk Environment |
| | | is associated with | IAM role |
| | `AWS::ElasticBeanstalk::ApplicationVersion` | is contained in | Elastic Beanstalk Application |
| | | is associated with | Elastic Beanstalk Environment |
| | | | S3 bucket |
| | `AWS::ElasticBeanstalk::Environment` | is contained in | Elastic Beanstalk Application |
| | | is associated with | Elastic Beanstalk Application Version |
| | | | IAM role |
| | | contains | CloudFormation Stack |

## AWS Entity Resolution

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Entity Resolution | `AWS::EntityResolut` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `ion::IdMappingWorkflow` | | |
| | `AWS::EntityResolution::MatchingWorkflow` | NA | NA |
| | `AWS::EntityResolution::SchemaMapping` | NA | NA |

## AWS Fault Injection Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Fault Injection Service | `AWS::FIS::ExperimentTemplate` | NA | NA |

## AWS Global Accelerator

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Global Accelerator | `AWS::GlobalAccelerator::Listener` | NA | NA |
| | `AWS::GlobalAccelerator::EndpointGroup` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | `AWS::GlobalAccelerator::Accelerator` | NA | NA |

## AWS Glue

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Glue | `AWS::Glue::Job` | NA | NA |
| | `AWS::Glue::Classifier` | NA | NA |
| | `AWS::Glue::MLTransform` | NA | NA |
| | `AWS::Glue::Database` | NA | NA |

## AWS Ground Station

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Ground Station | `AWS::GroundStation::Config` | NA | NA |
| | `AWS::GroundStation::MissionProfile` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | `AWS::GroundStation::DataflowEndpointGroup` | NA | NA |

## AWS HealthLake

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS HealthLake | `AWS::HealthLake::FHIRDatastore` | NA | NA |

## AWS Identity and Access Management (IAM)

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Identity and Access Management | `AWS::IAM::User` | is attached to | IAM group |
| | | | IAM customer managed policy |
| | `AWS::IAM::Group` | contains | IAM user |
| | | is attached to | IAM customer managed policy |
| | `AWS::IAM::Role` | is attached to | IAM customer managed policy |
| | `AWS::IAM::Policy` | is attached to | IAM user |
| | | | IAM group |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | | | IAM role |
| | `AWS::IAM::SAMLProvider` | NA | NA |
| | `AWS::IAM::ServerCertificate` | NA | NA |
| | `AWS::IAM::InstanceProfile` | NA | NA |
| | `AWS::IAM::OIDCProvider` | NA | NA |
| AWS Identity and Access Management Access Analyzer | `AWS::AccessAnalyzer::Analyzer` | NA | NA |
| AWS Identity and Access Management Roles Anywhere | `AWS::RolesAnywhere::Profile` | NA | NA |
| | `AWS::RolesAnywhere::TrustAnchor` | NA | NA |

AWS Config includes inline policies with the configuration details that it records. For more information on inline policies, see Managed policies and inline policies in the IAM User Guide.

# AWS IoT

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS IoT | AWS::IoT::AccountAuditConfiguration | NA | NA |
| | AWS::IoT::Authorizer | NA | NA |
| | AWS::IoT::CACertificate | NA | NA |
| | AWS::IoT::CustomMetric | NA | NA |
| | AWS::IoT::Dimension | NA | NA |
| | AWS::IoT::DomainConfiguration | NA | NA |
| | AWS::IoT::JobTemplate | NA | NA |
| | AWS::IoT::MitigationAction | NA | NA |
| | AWS::IoT::Policy | NA | NA |
| | AWS::IoT::ProvisioningTemplate | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::IoT::RoleAlias` | NA | NA |
| | `AWS::IoT::ScheduledAudit` | NA | NA |
| | `AWS::IoT::SecurityProfile` | NA | NA |
| | `AWS::IoT::ThingGroup` | NA | NA |
| | `AWS::IoTSiteWise::Gateway` | NA | NA |
| AWS IoT Wireless | `AWS::IoTWireless::ServiceProfile` | NA | NA |
| | `AWS::IoTWireless::MulticastGroup` | NA | NA |
| | `AWS::IoTWireless::FuotaTask` | NA | NA |
| AWS IoT Core | `AWS::IoT::FleetMetric` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS IoT Core Device Advisor | `AWS::IoTCoreDeviceAdvisor::SuiteDefinition` | NA | NA |
| AWS IoT Analytics | `AWS::IoTAnalytics::Datastore` | NA | NA |
| | `AWS::IoTAnalytics::Dataset` | NA | NA |
| | `AWS::IoTAnalytics::Pipeline` | NA | NA |
| | `AWS::IoTAnalytics::Channel` | NA | NA |
| AWS IoT Events | `AWS::IoTEvents::Input` | NA | NA |
| | `AWS::IoTEvents::DetectorModel` | NA | NA |
| | `AWS::IoTEvents::AlarmModel` | NA | NA |
| AWS IoT TwinMaker | `AWS::IoTTwinMaker::Workspace` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::IoTTwinMaker::Entity` | NA | NA |
| | `AWS::IoTTwinMaker::Scene` | NA | NA |
| | `AWS::IoTTwinMaker::SyncJob` | NA | NA |
| | `AWS::IoTTwinMaker::ComponentType` | NA | NA |
| AWS IoT SiteWise | `AWS::IoTSiteWise::Asset` | NA | NA |
| | `AWS::IoTSiteWise::AssetModel` | NA | NA |
| | `AWS::IoTSiteWise::Dashboard` | NA | NA |
| | `AWS::IoTSiteWise::Portal` | NA | NA |
| | `AWS::IoTSiteWise::Project` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS IoT Greengrass Version 2 | `AWS::GreengrassV2::ComponentVersion` | NA | NA |

## AWS Key Management Service

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Key Management Service | `AWS::KMS::Key` | NA | NA |
| | `AWS::KMS::Alias` | NA | NA |

## AWS Lambda

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Lambda | `AWS::Lambda::Function` | is associated with | IAM role |
| | | | EC2 security group |
| | | is contained in | EC2 subnet |
| | `AWS::Lambda::CodeSigningConfig` | NA | NA |

## AWS Mainframe Modernization

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Mainframe Modernization | `AWS::M2::Environment` | NA | NA |

## AWS Network Firewall

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Network Firewall | `AWS::NetworkFirewall::Firewall` | is attached to | EC2 Subnet |
| | | is associated with | NetworkFirewall FirewallPolicy |
| | `AWS::NetworkFirewall::FirewallPolicy` | is associated with | NetworkFirewall RuleGroup |
| | `AWS::NetworkFirewall::RuleGroup` | NA | NA |
| | `AWS::NetworkFirewall::TLSInspectionConfiguration` | NA | NA |
| | `AWS::NetworkFirewall::VpcEndpointAssociation` | NA | NA |

## AWS Network Manager

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Network Manager | `AWS::NetworkManager::Transi` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | tGatewayRegistration | | |
| | AWS::NetworkManager::Site | NA | NA |
| | AWS::NetworkManager::Device | NA | NA |
| | AWS::NetworkManager::Link | NA | NA |
| | AWS::NetworkManager::GlobalNetwork | NA | NA |
| | AWS::NetworkManager::CustomerGatewayAssociation | NA | NA |
| | AWS::NetworkManager::LinkAssociation | NA | NA |
| | AWS::NetworkManager::ConnectPeer | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | `AWS::NetworkManager::TransitGatewayPeering` | NA | NA |

## AWS Organizations

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Organizations | `AWS::Organizations::OrganizationalUnit` | NA | NA |

## AWS Panorama

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Panorama | `AWS::Panorama::Package` | NA | NA |

## AWS Private Certificate Authority

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Private Certificate Authority | `AWS::ACMPCA::CertificateAuthority` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::ACMPCA::CertificateAuthorityActivation` | NA | NA |
| AWS Private CA Connector for Active Directory | `AWS::PCAConnectorAD::Connector` | NA | NA |
| | `AWS::PCAConnectorAD::DirectoryRegistration` | NA | NA |

## AWS Resilience Hub

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Resilience Hub | `AWS::ResilienceHub::ResiliencyPolicy` | NA | NA |
| | `AWS::ResilienceHub::App` | NA | NA |

## AWS Resource Explorer

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Resource Explorer | `AWS::ResourceExplorer2::Index` | NA | NA |

## AWS RoboMaker

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS RoboMaker | `AWS::RoboMaker::RobotApplicationVersion` | NA | NA |
| | `AWS::RoboMaker::RobotApplication` | NA | NA |
| | `AWS::RoboMaker::SimulationApplication` | NA | NA |

## AWS Signer

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| AWS Signer | `AWS::Signer::SigningProfile` | NA | NA |

## AWS Secrets Manager

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Secrets Manager | `AWS::SecretsManager::Secret` | is associated with | Lambda function |
| | | is associated with | KMS Key |
| | `AWS::SecretsManager::ResourcePolicy` | NA | NA |
| | `AWS::SecretsManager::RotationSchedule` | NA | NA |

## AWS Security Hub CSPM

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Security Hub CSPM | `AWS::SecurityHub::Standard` | NA | NA |

## AWS Service Catalog

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Service Catalog | `AWS::ServiceCatalog::CloudFormationProduct` | is contained in | Portfolio |
| | | is associated with | CloudFormationProvisionedProduct |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::ServiceCatalog::CloudFormationProvisionedProduct` | is associated with | Portfolio |
| | | | CloudFormationProduct |
| | | | CloudFormationStack |
| | `AWS::ServiceCatalog::Portfolio` | contains | CloudFormationProduct |

> **Note**
>
> When you use AWS Service Catalog with AWS Config, configuration items show the child provisioned product's ARN instead of the parent product's ARN. This happens when a AWS Service Catalog provisioned product serves as a resource within a parent provisioned product through CloudFormation. The resource ID remains trackable through the AWS Config interfaces.

## AWS Shield

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Shield | `AWS::Shield::Protection` | is associated with | Amazon CloudFront distribution |
| | `AWS::ShieldRegional::Protection` | is associated with | EC2 EIP |
| | | is associated with | ElasticLoadBalancing Balancer |
| | | is associated with | ElasticLoadBalancingV2 LoadBalancer |

## AWS Step Functions

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Step Functions | `AWS::StepFunctions::Activity` | NA | NA |
| | `AWS::StepFunctions::StateMachine` | NA | NA |

## AWS Systems Manager

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Systems Manager | `AWS::SSM::ManagedInstanceInventory` * | is associated with | EC2 instance |
| | `AWS::SSM::PatchCompliance` | is associated with | Managed Instance Inventory |
| | `AWS::SSM::AssociationCompliance` | is associated with | Managed Instance Inventory |
| | `AWS::SSM::FileData` | is associated with | Managed Instance Inventory |
| | `AWS::SSM::Document` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::SSM::Resource DataSync` | NA | NA |
| AWS Systems Manager Incident Manager | `AWS::SSMIncidents::ResponsePlan` | NA | NA |
| AWS Systems Manager Incident Manager Contacts | `AWS::SSMContacts::Contact` | NA | NA |

*To learn more about managed instance inventory, see Recording Software Configuration for Managed Instances.

## AWS Transfer Family

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Transfer Family | `AWS::Transfer::Agreement` | NA | NA |
| | `AWS::Transfer::Connector` | NA | NA |
| | `AWS::Transfer::Workflow` | NA | NA |
| | `AWS::Transfer::Certificate` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::Transfer::Profile` | NA | NA |
| | `AWS::Transfer::Server` | NA | NA |

## AWS WAF

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS WAF | `AWS::WAF::RateBasedRule` | NA | NA |
| | `AWS::WAF::Rule` | NA | NA |
| | `AWS::WAF::WebACL` | is associated with | WAF Rule |
| | | | WAF rate based rule |
| | | | WAF Rulegroup |
| | `AWS::WAF::RuleGroup` | is associated with | WAF Rule |
| | `AWS::WAFRegional::RateBasedRule` | NA | NA |
| | `AWS::WAFRegional::Rule` | NA | NA |
| | `AWS::WAFRegional::WebACL` | is associated with | ElasticLoadBalancingV2 LoadBalancer |
| | | | WAFRegional Rule |

| AWS Service | Resource Type Value | Relationship | Related Resource |
| --- | --- | --- | --- |
| | | | WAFRegional rate based rule |
| | | | WAFRegional Rulegroup |
| | `AWS::WAFRegional::RuleGroup` | is associated with | WAFRegional Rule |
| AWS WAF V2 | `AWS::WAFv2::WebACL` | is associated with | ElasticLoadBalancingV2 LoadBalancer |
| | | | ApiGateway Stage |
| | | | WAFv2 IPSet |
| | | | WAFv2 RegexPatternSet |
| | | | WAFv2 RuleGroup |
| | | | WAFv2 ManagedRuleSet |
| | `AWS::WAFv2::RuleGroup` | is associated with | WAFv2 IPSet |
| | | | WAFv2 RegexPatternSet |
| | `AWS::WAFv2::ManagedRuleSet` | is associated with | WAFv2 RuleGroup |
| | `AWS::WAFv2::IPSet` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `AWS::WAFv2::RegexPatternSet` | NA | NA |

## AWS X-Ray

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS X-Ray | `AWS::XRay::EncryptionConfig` | NA | NA |

## Elastic Load Balancing

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| Elastic Load Balancing | Application Load Balancer<br><br>`AWS::ElasticLoadBalancingV2::LoadBalancer` | is associated with | EC2 security group |
| | | is attached to | Subnet |
| | | is contained in | Virtual private cloud (VPC) |
| | Application Load Balancer Listener<br><br>`AWS::ElasticLoadBalancingV2::Listener` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | Application Load Balancer Target Group<br><br>`AWS::ElasticLoadBalancingV2::TargetGroup` | NA | NA |
| | Classic Load Balancer<br><br>`AWS::ElasticLoadBalancing::LoadBalancer` | is associated with | EC2 security group |
| | | is attached to | Subnet |
| | | is contained in | Virtual private cloud (VPC) |
| | Network Load Balancer<br><br>`AWS::ElasticLoadBalancingV2::LoadBalancer` | NA | NA |

## AWS Elemental MediaConnect

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Elemental MediaConnect | `AWS::MediaConnect::FlowEntitlement` | NA | NA |
| | `AWS::MediaConnect:` | NA | NA |

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| | `:FlowVpcInterface` | | |
| | `AWS::MediaConnect::FlowSource` | NA | NA |
| | `AWS::MediaConnect::Gateway` | NA | NA |

## AWS Elemental MediaPackage

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Elemental MediaPackage | `AWS::MediaPackage::PackagingGroup` | NA | NA |
| | `AWS::MediaPackage::PackagingConfiguration` | NA | NA |
| AWS Elemental MediaPackage V2 | `AWS::MediaPackageV2::Channel` | NA | NA |
| | `AWS::MediaPackageV2::OriginEndpoint` | NA | NA |

## AWS Elemental MediaTailor

| AWS Service | Resource Type Value | Relationship | Related Resource |
|---|---|---|---|
| AWS Elemental MediaTailor | `AWS::MediaTailor::LiveSource` | NA | NA |
| | `AWS::MediaTailor::PlaybackConfiguration` | NA | NA |

# Resource Coverage by Region Availability

## North and South America Regions

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::ACM::Certificate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ACMPCA::CertificateAuthority | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ACMPCA::CertificateAuthorityActivation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::APS::RuleGroupsNamespace | No | Yes | Yes | Yes | No | No | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::AccessAnalyzer::Analyzer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AmazonMQ::Broker | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Amplify::App | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Amplify::Branch | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ApiGateway::DomainName | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::Method | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::RestApi | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::Stage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::UsagePlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Api | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Integration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::ApiGatewayV2::Stage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::Application | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppConfig::ConfigurationProfile | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppConfig::DeploymentStrategy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::Environment | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppConfig::Extension | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::ExtensionAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::HostedConfigurationVersion | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppFlow::Flow | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppIntegrations::Application | No | Yes | Yes | No | No | Yes | No | No |
| AWS::AppIntegrations::DataIntegration | No | Yes | Yes | No | No | Yes | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::AppIntegrations::EventIntegration | No | Yes | Yes | No | No | Yes | No | No |
| AWS::AppMesh::GatewayRoute | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppMesh::Mesh | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppMesh::Route | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppMesh::VirtualGateway | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppMesh::VirtualNode | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppMesh::VirtualRouter | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppMesh::VirtualService | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppRunner::Service | No | Yes | Yes | Yes | No | No | No | No |
| AWS::AppRunner::VpcConnector | No | Yes | Yes | Yes | No | No | No | No |
| AWS::AppStream::AppBlockBuilder | No | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::AppStream::Application | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppStream::DirectoryConfig | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppStream::Fleet | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::AppStream::Stack | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::AppSync::Api | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::AppSync::ApiCache | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::AppSync::GraphQLApi | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Athena::DataCatalog | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Athena::PreparedStatement | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Athena::WorkGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AuditManager::Assessment | Yes | Yes | Yes | Yes | No | Yes | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::AutoScaling::AutoScalingGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::LaunchConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::ScalingPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::ScheduledAction | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Auto Scaling::WarmPool | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::B2BI::Capability | No | Yes | Yes | Yes | No | No | No | No |
| AWS::B2BI::Profile | No | Yes | Yes | Yes | No | No | No | No |
| AWS::BCMDataExports::Export | No | Yes | No | No | No | No | No | No |
| AWS::Backup::BackupPlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Backup::BackupSelection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Backup::BackupVault | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Backup::RecoveryPoint | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::Backup::ReportPlan | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Backup::RestoreTestingPlan | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::BackupGateway::Hypervisor | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Batch::ComputeEnvironment | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Batch::JobQueue | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Batch::SchedulingPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Bedrock::ApplicationInferenceProfile | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Bedrock::Guardrail | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Bedrock::KnowledgeBase | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Bedrock::Prompt | No | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::BedrockAgentCore::BrowserCustom | No | Yes | Yes | Yes | No | No | No | No |
| AWS::BedrockAgentCore::CodeInterpreterCustom | No | Yes | Yes | Yes | No | No | No | No |
| AWS::BedrockAgentCore::Runtime | No | Yes | Yes | Yes | No | No | No | No |
| AWS::Budgets::BudgetsAction | No | Yes | No | No | No | No | No | No |
| AWS::Cassandra::Keyspace | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CleanRoomsML::TrainingDataset | No | Yes | Yes | Yes | No | No | No | No |
| AWS::Cloud9::EnvironmentEC2 | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CloudFormation::GuardHook | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::LambdaHook | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::Stack | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::StackSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::CloudFront::Distribution | No | Yes | No | No | No | No | No | No |
| AWS::CloudFront::KeyValueStore | No | Yes | No | No | No | No | No | No |
| AWS::CloudFront::PublicKey | No | Yes | No | No | No | No | No | No |
| AWS::CloudFront::RealtimeLogConfig | No | Yes | No | No | No | No | No | No |
| AWS::CloudFront::StreamingDistribution | No | Yes | No | No | No | No | No | No |
| AWS::CloudTrail::EventDataStore | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CloudTrail::Trail | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::Alarm | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::MetricStream | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CodeArtifact::Domain | No | Yes | Yes | Yes | No | No | No | No |
| AWS::CodeArtifact::Repository | No | Yes | Yes | Yes | No | No | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::CodeBuild::Project | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CodeBuild::ReportGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CodeDeploy::Application | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CodeDeploy::DeploymentConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CodeDeploy::DeploymentGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::CodeGuruProfiler::ProfilingGroup | No | Yes | Yes | Yes | No | No | No | No |
| AWS::CodeGuruReviewer::RepositoryAssociation | No | Yes | Yes | Yes | No | No | No | No |
| AWS::CodePipeline::Pipeline | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Cognito::IdentityPool | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Cognito::UserPool | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Cognito::UserPoolClient | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Cognito::UserPoolGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Comprehend::Flywheel | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Config::AggregationAuthorization | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ConfigurationRecorder | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ConformancePack | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::Config::ConformancePackCompliance | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::Config::ResourceCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::StoredQuery | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Connect::Instance | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Connect::PhoneNumber | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Connect::QuickConnect | No | Yes | Yes | No | No | Yes | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Connect::Rule | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Connect::SecurityProfile | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Connect::User | No | Yes | Yes | No | No | Yes | No | No |
| AWS::CustomerProfiles::Domain | No | Yes | Yes | No | No | Yes | No | No |
| AWS::CustomerProfiles::ObjectType | No | Yes | Yes | No | No | Yes | No | No |
| AWS::DMS::Certificate | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DMS::Endpoint | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DMS::EventSubscription | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DMS::MigrationProject | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::DMS::ReplicationInstance | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DMS::ReplicationSubnetGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::DMS::ReplicationTask | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DataSync::Agent | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationEFS | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DataSync::LocationFSxLustre | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DataSync::LocationFSxWindows | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DataSync::LocationHDFS | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::DataSync::LocationNFS | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::DataSync::LocationObjectStorage | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::DataSync::LocationS3 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationSMB | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::DataSync::Task | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Deadline::Fleet | No | Yes | Yes | Yes | No | No | No | No |
| AWS::Deadline::Monitor | No | Yes | Yes | Yes | No | No | No | No |
| AWS::Deadline::QueueFleetAssociation | No | Yes | Yes | Yes | No | No | No | No |
| AWS::Detective::Graph | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::DeviceFarm::InstanceProfile | No | No | Yes | No | No | No | No | No |
| AWS::DeviceFarm::Project | No | No | Yes | No | No | No | No | No |
| AWS::DeviceFarm::TestGridProject | No | No | Yes | No | No | No | No | No |
| AWS::DynamoDB::Table | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::Capacity Reservation | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::CarrierGateway | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::EC2::ClientVpnEndpoint | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::ClientVpnTargetNetworkAssociation | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::CustomerGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::DHCPOptions | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::EC2Fleet | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::EIP | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::EIPAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::EgressOnlyInternetGateway | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::FlowLog | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::Host | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAM | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::IPAMPool | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::IPAMPoolCidr | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::IPAMResourceDiscovery | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::IPAMResourceDiscoveryAssociation | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::IPAMScope | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::Instance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::InstanceConnectEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::InternetGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::LaunchTemplate | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::NatGateway | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::NetworkAcl | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::NetworkInsightsAccessScope | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::NetworkInsightsAccessScopeAnalysis | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::EC2::NetworkInsightsAnalysis | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::NetworkInsightsPath | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::EC2::NetworkInterface | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::PrefixList | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::RouteTable | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SecurityGroupVpcAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SnapshotBlockPublicAccess | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SpotFleet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::Subnet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::SubnetCidrBlock | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetNetworkAclAssociation | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::EC2::SubnetRouteTableAssociation | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::EC2::TrafficMirrorFilter | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::TrafficMirrorSession | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::EC2::TrafficMirrorTarget | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::EC2::TransitGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::TransitGatewayAttachment | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::TransitGatewayConnect | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::TransitGatewayMulticastDomain | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::TransitGatewayRouteTable | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::VPC | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessExclusion | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::VPCBlockPublicAccessOptions | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::VPCEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpointConnectionNotification | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpointService | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCGatewayAttachment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCPeeringConnection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNConnection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNConnectionRoute | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::VerifiedAccessInstance | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EC2::Volume | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::PublicRepository | No | Yes | No | No | No | No | No | No |
| AWS::ECR::PullThroughCacheRule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::RegistryPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::ReplicationConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::Repository | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::RepositoryCreationTemplate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::CapacityProvider | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::Service | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::ECS::TaskDefinition | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::TaskSet | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EFS::AccessPoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EFS::FileSystem | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EKS::Addon | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EKS::Cluster | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::EKS::FargateProfile | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EKS::IdentityProviderConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EMR::SecurityConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EMR::Studio | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EMRContainers::VirtualCluster | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EMRServerless::Application | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ElasticBeanstalk::Application | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::ElasticBeanstalk::ApplicationVersion | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::ElasticBeanstalk::Environment | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::ElasticLoadBalancing::LoadBalancer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::Listener | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::LoadBalancer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::TargetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Elasticsearch::Domain | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EntityResolution::IdMappingWorkflow | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::EntityResolution::MatchingWorkflow | No | Yes | Yes | Yes | No | Yes | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::EntityResolution::SchemaMapping | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::EventSchemas::Discoverer | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EventSchemas::Registry | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EventSchemas::RegistryPolicy | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::EventSchemas::Schema | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Events::ApiDestination | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Events::Archive | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Events::Connection | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Events::Endpoint | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Events::EventBus | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Events::Rule | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::FIS::ExperimentTemplate | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Forecast::Dataset | No | Yes | Yes | Yes | No | No | No | No |
| AWS::Forecast::DatasetGroup | No | Yes | Yes | Yes | No | No | No | No |
| AWS::FraudDetector::EntityType | No | Yes | Yes | Yes | No | No | No | No |
| AWS::FraudDetector::Label | No | Yes | Yes | Yes | No | No | No | No |
| AWS::FraudDetector::Outcome | No | Yes | Yes | Yes | No | No | No | No |
| AWS::FraudDetector::Variable | No | Yes | Yes | Yes | No | No | No | No |
| AWS::GameLift::Alias | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::GameLift::Build | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::GameLift::GameSessionQueue | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::GameLift::MatchmakingConfiguration | No | Yes | Yes | No | No | No | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::GlobalAccelerator::Accelerator | No | No | Yes | No | No | No | No | No |
| AWS::GlobalAccelerator::EndpointGroup | No | No | Yes | No | No | No | No | No |
| AWS::GlobalAccelerator::Listener | No | No | Yes | No | No | No | No | No |
| AWS::Glue::Classifier | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Glue::Database | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Glue::Job | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::Glue::MLTransform | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Glue::Registry | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Grafana::Workspace | No | Yes | Yes | Yes | No | No | No | No |
| AWS::GreengrassV2::ComponentVersion | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::GroundStation::Config | No | Yes | Yes | Yes | No | No | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::GroundStation::DataflowEndpointGroup | No | Yes | Yes | Yes | No | No | No | Yes |
| AWS::GroundStation::MissionProfile | No | Yes | Yes | Yes | No | No | No | Yes |
| AWS::GuardDuty::Detector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::GuardDuty::Filter | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::GuardDuty::IPSet | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::GuardDuty::MalwareProtectionPlan | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::GuardDuty::ThreatIntelSet | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::HealthLake::FHIRDatastore | No | Yes | Yes | Yes | No | No | No | No |
| AWS::IAM::Group | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IAM::InstanceProfile | No | Yes | No | No | No | No | No | No |
| AWS::IAM::OIDCProvider | No | Yes | No | No | No | No | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::IAM::Policy | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IAM::Role | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IAM::SAMLProvider | No | Yes | No | No | No | No | No | No |
| AWS::IAM::ServerCertificate | No | Yes | No | No | No | No | No | No |
| AWS::IAM::User | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IVS::Channel | No | Yes | Yes | No | No | No | No | No |
| AWS::IVS::PlaybackKeyPair | No | Yes | Yes | No | No | No | No | No |
| AWS::IVS::RecordingConfiguration | No | Yes | Yes | No | No | No | No | No |
| AWS::ImageBuilder::ContainerRecipe | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::DistributionConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::ImagePipeline | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::ImageBuilder::ImageRecipe | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::InfrastructureConfiguration | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ImageBuilder::LifecyclePolicy | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::InspectorV2::Activation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::InspectorV2::Filter | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::IoT::AccountAuditConfiguration | Yes | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoT::Authorizer | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoT::CACertificate | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoT::CustomMetric | Yes | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoT::Dimension | Yes | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoT::DomainConfiguration | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoT::FleetMetric | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoT::JobTemplate | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoT::MitigationAction | Yes | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoT::Policy | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoT::ProvisioningTemplate | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoT::RoleAlias | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoT::ScheduledAudit | Yes | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoT::SecurityProfile | Yes | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoT::ThingGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::IoTAnalytics::Channel | No | Yes | Yes | Yes | No | No | No | No |
| AWS::IoTAnalytics::Dataset | No | Yes | Yes | Yes | No | No | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoTAnalytics::Datastore | No | Yes | Yes | Yes | No | No | No | No |
| AWS::IoTAnalytics::Pipeline | No | Yes | Yes | Yes | No | No | No | No |
| AWS::IoTCoreDeviceAdvisor::SuiteDefinition | No | Yes | Yes | No | No | No | No | No |
| AWS::IoTEvents::AlarmModel | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTEvents::DetectorModel | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTEvents::Input | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTSiteWise::Asset | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTSiteWise::AssetModel | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTSiteWise::Dashboard | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTSiteWise::Gateway | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTSiteWise::Portal | No | Yes | Yes | Yes | No | Yes | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoTSiteWise::Project | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::IoTTwinMaker::ComponentType | No | Yes | Yes | No | No | No | No | No |
| AWS::IoTTwinMaker::Entity | No | Yes | Yes | No | No | No | No | No |
| AWS::IoTTwinMaker::Scene | No | Yes | Yes | No | No | No | No | No |
| AWS::IoTTwinMaker::SyncJob | No | Yes | Yes | No | No | No | No | No |
| AWS::IoTTwinMaker::Workspace | No | Yes | Yes | No | No | No | No | No |
| AWS::IoTWireless::FuotaTask | No | Yes | Yes | No | No | No | No | Yes |
| AWS::IoTWireless::MulticastGroup | No | Yes | Yes | No | No | No | No | Yes |
| AWS::IoTWireless::ServiceProfile | No | Yes | Yes | No | No | No | No | Yes |
| AWS::KMS::Alias | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::KMS::Key | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::KafkaConnect::Connector | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::KafkaConnect::CustomPlugin | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::Kendra::Index | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Kinesis::Stream | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::Kinesis::StreamConsumer | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::KinesisAnalyticsV2::Application | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::KinesisFirehose::DeliveryStream | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::KinesisVideo::SignalingChannel | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::KinesisVideo::Stream | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Lambda::CodeSigningConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Lambda::Function | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Lex::Bot | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Lex::BotAlias | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Lightsail::Bucket | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Lightsail::Certificate | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Lightsail::Disk | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Lightsail::StaticIp | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Location::APIKey | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Location::GeofenceCollection | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Location::Map | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Location::PlaceIndex | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Location::RouteCalculator | No | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Logs::Destination | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::LookoutVision::Project | No | Yes | Yes | Yes | No | No | No | No |
| AWS::M2::Environment | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MSK::BatchScramSecret | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MSK::Cluster | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MSK::ClusterPolicy | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MSK::Configuration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::MSK::ServerlessCluster | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::MSK::VpcConnection | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Macie::Session | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaConnect::FlowEntitlement | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::MediaConnect::FlowSource | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaConnect::FlowVpcInterface | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaConnect::Gateway | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaLive::Multiplexprogram | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaPackage::Asset | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaPackage::PackagingConfiguration | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaPackage::PackagingGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaPackageV2::Channel | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaPackageV2::ChannelGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaPackageV2::OriginEndpoint | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MediaTailor::LiveSource | No | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::MediaTailor::PlaybackConfiguration | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::MemoryDB::SubnetGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::NetworkFirewall::Firewall | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::FirewallPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::RuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::TLSInspectionConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::VpcEndpointAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkManager::ConnectPeer | No | No | Yes | No | No | No | No | No |
| AWS::NetworkManager::CustomerGatewayAssociation | No | No | Yes | No | No | No | No | No |
| AWS::NetworkManager::Device | No | No | Yes | No | No | No | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::NetworkManager::GlobalNetwork | No | No | Yes | No | No | No | No | No |
| AWS::NetworkManager::Link | No | No | Yes | No | No | No | No | No |
| AWS::NetworkManager::LinkAssociation | No | No | Yes | No | No | No | No | No |
| AWS::NetworkManager::Site | No | No | Yes | No | No | No | No | No |
| AWS::NetworkManager::TransitGatewayPeering | No | No | Yes | No | No | No | No | No |
| AWS::NetworkManager::TransitGatewayRegistration | No | No | Yes | No | No | No | No | No |
| AWS::Omics::RunGroup | No | Yes | Yes | No | No | No | No | No |
| AWS::Omics::Workflow | No | Yes | Yes | No | No | No | No | No |
| AWS::OpenSearch::Domain | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::OpenSearchServerless::Collection | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::OpenSearchServerless::SecurityConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::OpenSearchServerless::VpcEndpoint | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::PCAConnectorAD::Connector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::PCAConnectorAD::DirectoryRegistration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Panorama::Package | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Personalize::Dataset | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Personalize::DatasetGroup | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Personalize::Schema | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Personalize::Solution | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Pinpoint::App | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Pinpoint::ApplicationSettings | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Pinpoint::Campaign | No | Yes | Yes | No | No | Yes | No | No |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Pinpoint::EmailChannel | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Pinpoint::EmailTemplate | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Pinpoint::EventStream | No | Yes | Yes | No | No | Yes | No | No |
| AWS::Pinpoint::InAppTemplate | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::Pinpoint::Segment | No | Yes | Yes | No | No | Yes | No | No |
| AWS::QuickSight::Dashboard | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::QuickSight::DataSource | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::QuickSight::Template | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::QuickSight::Theme | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::RDS::DBCluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBClusterSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::RDS::DBInstance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBProxyEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSubnetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::EventSubscription | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::GlobalCluster | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::RDS::Integration | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::RDS::OptionGroup | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::RUM::AppMonitor | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Redshift::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Redshift::ClusterParameterGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSubnetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::EndpointAccess | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Redshift::EndpointAuthorization | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Redshift::EventSubscription | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::Integration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ScheduledAction | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ResilienceHub::App | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ResilienceHub::ResiliencyPolicy | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::ResourceExplorer2::Index | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RoboMaker::RobotApplication | No | Yes | Yes | Yes | No | No | No | No |
| AWS::RoboMaker::RobotApplicationVersion | No | Yes | Yes | Yes | No | No | No | No |
| AWS::RoboMaker::SimulationApplication | No | Yes | Yes | Yes | No | No | No | No |
| AWS::RolesAnywhere::CRL | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RolesAnywhere::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RolesAnywhere::TrustAnchor | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53::DNSSEC | No | Yes | No | No | No | No | No | No |
| AWS::Route53::HealthCheck | No | Yes | No | No | No | No | No | No |
| AWS::Route53::HostedZone | No | Yes | No | No | No | No | No | No |
| AWS::Route53Profiles::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Route53Profiles::ProfileAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53RecoveryControl::Cluster | No | No | Yes | No | No | No | No | No |
| AWS::Route53RecoveryControl::ControlPanel | No | No | Yes | No | No | No | No | No |
| AWS::Route53RecoveryControl::RoutingControl | No | No | Yes | No | No | No | No | No |
| AWS::Route53RecoveryControl::SafetyRule | No | No | Yes | No | No | No | No | No |
| AWS::Route53RecoveryReadiness::Cell | No | No | Yes | No | No | No | No | No |
| AWS::Route53RecoveryReadiness::ReadinessCheck | No | No | Yes | No | No | No | No | No |
| AWS::Route53RecoveryReadiness::RecoveryGroup | No | No | Yes | No | No | No | No | No |
| AWS::Route53RecoveryReadiness::ResourceSet | No | No | Yes | No | No | No | No | No |
| AWS::Route53Resolver::FirewallDomainList | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Route53Resolver::FirewallRuleGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverEndpoint | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverRule | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Route53Resolver::ResolverRuleAssociation | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::S3::AccessGrant | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::AccessGrantsInstance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::AccessGrantsLocation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::S3::AccessPoint | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::S3::AccountPublicAccessBlock | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::S3::Bucket | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::MultiRegionAccessPoint | No | No | Yes | No | No | No | No | No |
| AWS::S3::StorageLens | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::S3::StorageLensGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::S3Express::BucketPolicy | No | Yes | Yes | Yes | No | No | No | No |
| AWS::S3Express::DirectoryBucket | No | Yes | Yes | Yes | No | No | No | No |
| AWS::S3Tables::TableBucket | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3Tables::TableBucketPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SES::ConfigurationSet | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::SES::ContactList | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SES::DedicatedIpPool | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SES::MailManagerTrafficPolicy | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SES::ReceiptFilter | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SES::ReceiptRuleSet | No | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SES::Template | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SNS::Topic | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SQS::Queue | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SSM::AssociationCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::Document | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::FileData | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::SSM::ManagedInstanceInventory | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::PatchCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::ResourceDataSync | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSMContacts::Contact | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SSMIncidents::ResponsePlan | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::AppImageConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::CodeRepository | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::DataQualityJobDefinition | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::Domain | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::EndpointConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::FeatureGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::Image | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::InferenceExperiment | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::MlflowTrackingServer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SageMaker::Model | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::ModelBiasJobDefinition | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::ModelExplainabilityJobDefinition | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::ModelQualityJobDefinition | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::MonitoringSchedule | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::NotebookInstance | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::StudioLifecycleConfig | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::UserProfile | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::SageMaker::Workteam | No | Yes | Yes | Yes | No | Yes | No | No |
| AWS::SecretsManager::ResourcePolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::RotationSchedule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::Secret | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecurityHub::Standard | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProduct | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ServiceCatalog::Portfolio | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ServiceDiscovery::HttpNamespace | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::ServiceDiscovery::Instance | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::ServiceDiscovery::PublicDnsNamespace | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceDiscovery::Service | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::Shield::Protection | No | Yes | No | No | No | No | No | No |
| AWS::ShieldRegional::Protection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Signer::SigningProfile | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::Step Functions::Activity | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::StepFunctions::StateMachine | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Agreement | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |
| AWS::Transfer::Certificate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Connector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::Transfer::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Server | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Workflow | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAF::RateBasedRule | No | Yes | No | No | No | No | No | No |
| AWS::WAF::Rule | No | Yes | No | No | No | No | No | No |
| AWS::WAF::RuleGroup | No | Yes | No | No | No | No | No | No |
| AWS::WAF::WebACL | No | Yes | No | No | No | No | No | No |
| AWS::WAFRegional::RateBasedRule | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::WAFRegional::Rule | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::WAFRegional::RuleGroup | Yes | Yes | Yes | Yes | No | Yes | No | Yes |
| AWS::WAFRegional::WebACL | Yes | Yes | Yes | Yes | No | Yes | No | Yes |

| Resource type | US West (N. California) | US East (N. Virginia) | US West (Oregon) | US East (Ohio) | Canada West (Calgary) | Canada (Central) | Mexico (Central) | South America (São Paulo) |
|---|---|---|---|---|---|---|---|---|
| AWS::WAFv2::IPSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::ManagedRuleSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RegexPatternSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::WebACL | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WorkSpaces::ConnectionAlias | No | Yes | Yes | No | No | Yes | No | Yes |
| AWS::WorkSpaces::Workspace | No | Yes | Yes | No | No | Yes | No | Yes |
| AWS::XRay::EncryptionConfig | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes |

# Europe Regions

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::ACM::Certificate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ACMPCA::CertificateAuthority | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ACMPCA::CertificateAuthorityActivation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::APS::RuleGroupsNamespace | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::AccessAnalyzer::Analyzer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AmazonMQ::Broker | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::Amplify::App | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::Amplify::Branch | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::ApiGateway::DomainName | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::Method | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::RestApi | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::ApiGateway::Stage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::UsagePlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Api | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Integration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Stage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::Application | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppConfig::ConfigurationProfile | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppConfig::DeploymentStrategy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::Environment | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppConfig::Extension | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::ExtensionAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppConfig::HostedConfigurationVersion | Yes | Yes | Yes | Yes | Yes | Yes | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::AppFlow::Flow | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::AppIntegrations::Application | No | Yes | Yes | No | No | No | No | No |
| AWS::AppIntegrations::DataIntegration | No | Yes | Yes | No | No | No | No | No |
| AWS::AppIntegrations::EventIntegration | No | Yes | Yes | No | No | No | No | No |
| AWS::AppMesh::GatewayRoute | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppMesh::Mesh | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppMesh::Route | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppMesh::VirtualGateway | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppMesh::VirtualNode | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppMesh::VirtualRouter | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppMesh::VirtualService | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::AppRunner::Service | Yes | Yes | Yes | Yes | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::AppRunner::VpcConnector | Yes | Yes | No | Yes | No | No | No | No |
| AWS::AppStream::AppBlockBuilder | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::AppStream::Application | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::AppStream::DirectoryConfig | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::AppStream::Fleet | Yes | Yes | Yes | No | No | No | No | No |
| AWS::AppStream::Stack | Yes | Yes | Yes | No | No | No | No | No |
| AWS::AppSync::Api | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppSync::ApiCache | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AppSync::GraphQLApi | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Athena::DataCatalog | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Athena::PreparedStatement | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Athena::WorkGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::AuditManager::Assessment | Yes | Yes | Yes | No | No | No | No | No |
| AWS::AutoScaling::AutoScalingGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::LaunchConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::ScalingPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::ScheduledAction | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::WarmPool | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::BCMDataExports::Export | No | No | Yes | No | No | No | No | No |
| AWS::Backup::BackupPlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Backup::BackupSelection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Backup::BackupVault | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Backup::RecoveryPoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Backup::ReportPlan | Yes | Yes | Yes | Yes | Yes | Yes | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Backup::RestoreTestingPlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::BackupGateway::Hypervisor | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::Batch::ComputeEnvironment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Batch::JobQueue | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Batch::SchedulingPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Bedrock::ApplicationInferenceProfile | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::Bedrock::Guardrail | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Bedrock::KnowledgeBase | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Bedrock::Prompt | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::BedrockAgentCore::BrowserCustom | Yes | Yes | No | No | No | No | No | No |
| AWS::BedrockAgentCore::CodeInterpreterCustom | Yes | Yes | No | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::BedrockAgentCore::Runtime | Yes | Yes | No | No | No | No | No | No |
| AWS::Cassandra::Keyspace | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::CleanRoomsML::TrainingDataset | Yes | Yes | Yes | No | Yes | No | No | No |
| AWS::Cloud9::EnvironmentEC2 | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::CloudFormation::GuardHook | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::LambdaHook | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::Stack | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::CloudFormation::StackSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudTrail::EventDataStore | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudTrail::Trail | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::Alarm | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::MetricStream | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::CodeArtifact::Domain | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::CodeArtifact::Repository | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::CodeBuild::Project | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CodeBuild::ReportGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CodeDeploy::Application | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::CodeDeploy::DeploymentConfig | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::CodeDeploy::DeploymentGroup | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::CodeGuruProfiler::ProfilingGroup | Yes | Yes | Yes | No | Yes | No | No | No |
| AWS::CodeGuruReviewer::RepositoryAssociation | Yes | Yes | Yes | No | Yes | No | No | No |
| AWS::CodePipeline::Pipeline | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Cognito::IdentityPool | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Cognito::UserPool | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Cognito::UserPoolClient | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Cognito::UserPoolGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Comprehend::Flywheel | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Config::AggregationAuthorization | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ConfigurationRecorder | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ConformancePack | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ConformancePackCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ResourceCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::StoredQuery | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Connect::Instance | No | Yes | Yes | No | No | No | No | No |
| AWS::Connect::PhoneNumber | No | Yes | Yes | No | No | No | No | No |
| AWS::Connect::QuickConnect | No | Yes | Yes | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Connect::Rule | No | Yes | Yes | No | No | No | No | No |
| AWS::Connect::SecurityProfile | No | Yes | Yes | No | No | No | No | No |
| AWS::Connect::User | No | Yes | Yes | No | No | No | No | No |
| AWS::CustomerProfiles::Domain | No | Yes | Yes | No | No | No | No | No |
| AWS::CustomerProfiles::ObjectType | No | Yes | Yes | No | No | No | No | No |
| AWS::DMS::Certificate | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DMS::Endpoint | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DMS::EventSubscription | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DMS::MigrationProject | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DMS::ReplicationInstance | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DMS::ReplicationSubnetGroup | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DMS::ReplicationTask | Yes | Yes | Yes | Yes | Yes | Yes | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::DataSync::Agent | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationEFS | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationFSxLustre | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DataSync::LocationFSxWindows | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DataSync::LocationHDFS | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationNFS | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationObjectStorage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationS3 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationSMB | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::Task | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Deadline::Fleet | Yes | Yes | No | No | No | No | No | No |
| AWS::Deadline::Monitor | Yes | Yes | No | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Deadline::QueueFleetAssociation | Yes | Yes | No | No | No | No | No | No |
| AWS::Detective::Graph | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::DynamoDB::Table | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::Capacity Reservation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::CarrierGateway | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::EC2::ClientVpnEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::ClientVpnTargetNetworkAssociation | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::CustomerGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::DHCPOptions | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::EC2Fleet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::EIP | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::EIPAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::EgressOnlyInternetGateway | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::FlowLog | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::Host | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAM | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMPool | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMPoolCidr | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMResourceDiscovery | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMResourceDiscoveryAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMScope | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::Instance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::InstanceConnectEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::InternetGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::LaunchTemplate | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::EC2::NatGateway | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::NetworkAcl | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::NetworkInsightsAccessScope | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::EC2::NetworkInsightsAccessScopeAnalysis | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::EC2::NetworkInsightsAnalysis | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::EC2::NetworkInsightsPath | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::EC2::NetworkInterface | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::PrefixList | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::RouteTable | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::SecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SecurityGroupVpcAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SnapshotBlockPublicAccess | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SpotFleet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::Subnet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetCidrBlock | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetNetworkAclAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetRouteTableAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::TrafficMirrorFilter | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::TrafficMirrorSession | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::TrafficMirrorTarget | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::TransitGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::TransitGatewayAttachment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::TransitGatewayConnect | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::TransitGatewayMulticastDomain | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::TransitGatewayRouteTable | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::EC2::VPC | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessExclusion | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessOptions | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpointConnectionNotification | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpointService | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCGatewayAttachment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCPeeringConnection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::EC2::VPNConnection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNConnectionRoute | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VerifiedAccessInstance | Yes | Yes | Yes | No | Yes | Yes | No | No |
| AWS::EC2::Volume | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::PullThroughCacheRule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::RegistryPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::ReplicationConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::Repository | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::RepositoryCreationTemplate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::CapacityProvider | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::ECS::Service | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::TaskDefinition | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::TaskSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EFS::AccessPoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EFS::FileSystem | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EKS::Addon | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EKS::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EKS::FargateProfile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EKS::IdentityProviderConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EMR::SecurityConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EMR::Studio | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EMRContainers::VirtualCluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::EMRServerless::Application | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::ElasticBeanstalk::Application | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticBeanstalk::ApplicationVersion | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticBeanstalk::Environment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancing::LoadBalancer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::Listener | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::ElasticLoadBalancingV2::LoadBalancer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::TargetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Elasticsearch::Domain | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EntityResolution::IdMappingWorkflow | Yes | Yes | Yes | No | No | No | No | No |
| AWS::EntityResolution::MatchingWorkflow | Yes | Yes | Yes | No | No | No | No | No |
| AWS::EntityResolution::SchemaMapping | Yes | Yes | Yes | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::EventSchemas::Discoverer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EventSchemas::Registry | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EventSchemas::RegistryPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EventSchemas::Schema | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Events::ApiDestination | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Events::Archive | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Events::Connection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Events::Endpoint | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Events::EventBus | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Events::Rule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::FIS::ExperimentTemplate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| AWS::Forecast::Dataset | Yes | Yes | No | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Forecast::DatasetGroup | Yes | Yes | No | No | No | No | No | No |
| AWS::FraudDetector::EntityType | Yes | No | No | No | No | No | No | No |
| AWS::FraudDetector::Label | Yes | No | No | No | No | No | No | No |
| AWS::FraudDetector::Outcome | Yes | No | No | No | No | No | No | No |
| AWS::FraudDetector::Variable | Yes | No | No | No | No | No | No | No |
| AWS::GameLift::Alias | Yes | Yes | Yes | No | No | No | No | No |
| AWS::GameLift::Build | Yes | Yes | Yes | No | No | No | No | No |
| AWS::GameLift::GameSessionQueue | Yes | Yes | Yes | No | No | No | No | No |
| AWS::GameLift::MatchmakingConfiguration | Yes | Yes | No | No | No | No | No | No |
| AWS::Glue::Classifier | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Glue::Database | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Glue::Job | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Glue::MLTransform | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Glue::Registry | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::Grafana::Workspace | Yes | Yes | Yes | No | No | No | No | No |
| AWS::GreengrassV2::ComponentVersion | Yes | Yes | Yes | No | No | No | No | No |
| AWS::GroundStation::Config | Yes | Yes | No | No | Yes | No | No | No |
| AWS::GroundStation::DataflowEndpointGroup | Yes | Yes | No | No | Yes | No | No | No |
| AWS::GroundStation::MissionProfile | Yes | Yes | No | No | Yes | No | No | No |
| AWS::GuardDuty::Detector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::GuardDuty::Filter | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::GuardDuty::IPSet | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::GuardDuty::MalwareProtectionPlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::GuardDuty::ThreatIntelSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::HealthLake::FHIRDatastore | Yes | No | Yes | No | No | No | No | No |
| AWS::IAM::Group | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::IAM::Policy | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::IAM::Role | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::IAM::User | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::IVS::Channel | Yes | Yes | No | No | No | No | No | No |
| AWS::IVS::PlaybackKeyPair | Yes | Yes | No | No | No | No | No | No |
| AWS::IVS::RecordingConfiguration | Yes | Yes | No | No | No | No | No | No |
| AWS::ImageBuilder::ContainerRecipe | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::DistributionConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::ImagePipeline | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::ImageRecipe | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::ImageBuilder::InfrastructureConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::LifecyclePolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::InspectorV2::Activation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::InspectorV2::Filter | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::IoT::AccountAuditConfiguration | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::Authorizer | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::CACertificate | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::CustomMetric | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::Dimension | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::DomainConfiguration | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::FleetMetric | Yes | Yes | Yes | Yes | Yes | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoT::JobTemplate | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::MitigationAction | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::Policy | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::ProvisioningTemplate | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::RoleAlias | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::ScheduledAudit | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::SecurityProfile | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::IoT::ThingGroup | Yes | Yes | Yes | Yes | Yes | No | Yes | No |
| AWS::IoTAnalytics::Channel | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTAnalytics::Dataset | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTAnalytics::Datastore | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTAnalytics::Pipeline | Yes | Yes | No | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoTCoreDeviceAdvisor::SuiteDefinition | Yes | No | No | No | No | No | No | No |
| AWS::IoTEvents::AlarmModel | Yes | Yes | Yes | No | No | No | No | No |
| AWS::IoTEvents::DetectorModel | Yes | Yes | Yes | No | No | No | No | No |
| AWS::IoTEvents::Input | Yes | Yes | Yes | No | No | No | No | No |
| AWS::IoTSiteWise::Asset | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTSiteWise::AssetModel | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTSiteWise::Dashboard | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTSiteWise::Gateway | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTSiteWise::Portal | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTSiteWise::Project | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTTwinMaker::ComponentType | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTTwinMaker::Entity | Yes | Yes | No | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::IoTTwinMaker::Scene | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTTwinMaker::SyncJob | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTTwinMaker::Workspace | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTWireless::FuotaTask | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTWireless::MulticastGroup | Yes | Yes | No | No | No | No | No | No |
| AWS::IoTWireless::ServiceProfile | Yes | Yes | No | No | No | No | No | No |
| AWS::KMS::Alias | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::KMS::Key | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::KafkaConnect::Connector | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::KafkaConnect::CustomPlugin | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Kendra::Index | Yes | No | Yes | No | No | No | No | No |
| AWS::Kinesis::Stream | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Kinesis::StreamConsumer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::KinesisAnalyticsV2::Application | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::KinesisFirehose::DeliveryStream | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::KinesisVideo::SignalingChannel | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::KinesisVideo::Stream | Yes | Yes | Yes | Yes | No | No | No | No |
| AWS::Lambda::CodeSigningConfig | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::Lambda::Function | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Lex::Bot | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Lex::BotAlias | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Lightsail::Bucket | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Lightsail::Certificate | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Lightsail::Disk | Yes | Yes | Yes | Yes | Yes | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Lightsail::StaticIp | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Location::APIKey | Yes | Yes | Yes | No | Yes | No | No | No |
| AWS::Location::GeofenceCollection | Yes | Yes | Yes | No | Yes | No | Yes | No |
| AWS::Location::Map | Yes | Yes | Yes | No | Yes | No | Yes | No |
| AWS::Location::PlaceIndex | Yes | Yes | Yes | No | Yes | No | Yes | No |
| AWS::Location::RouteCalculator | Yes | Yes | Yes | No | Yes | No | Yes | No |
| AWS::Logs::Destination | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::LookoutVision::Project | Yes | Yes | No | No | No | No | No | No |
| AWS::M2::Environment | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::MSK::BatchScramSecret | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::MSK::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::MSK::ClusterPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::MSK::Configuration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::MSK::ServerlessCluster | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MSK::VpcConnection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Macie::Session | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::MediaConnect::FlowEntitlement | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaConnect::FlowSource | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaConnect::FlowVpcInterface | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaConnect::Gateway | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaLive::Multiplexprogram | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaPackage::Asset | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaPackage::PackagingConfiguration | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaPackage::PackagingGroup | Yes | Yes | Yes | Yes | Yes | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::MediaPackageV2::Channel | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaPackageV2::ChannelGroup | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaPackageV2::OriginEndpoint | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::MediaTailor::LiveSource | Yes | Yes | No | Yes | Yes | No | No | No |
| AWS::MediaTailor::PlaybackConfiguration | Yes | Yes | No | Yes | Yes | No | No | No |
| AWS::MemoryDB::SubnetGroup | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::NetworkFirewall::Firewall | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::FirewallPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::RuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::TLSInspectionConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::VpcEndpointAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Omics::RunGroup | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Omics::Workflow | Yes | Yes | Yes | No | No | No | No | No |
| AWS::OpenSearch::Domain | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::OpenSearchServerless::Collection | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::OpenSearchServerless::SecurityConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::OpenSearchServerless::VpcEndpoint | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::PCAConnectorAD::Connector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::PCAConnectorAD::DirectoryRegistration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Panorama::Package | Yes | No | No | No | No | No | No | No |
| AWS::Personalize::Dataset | Yes | Yes | No | No | No | No | No | No |
| AWS::Personalize::DatasetGroup | Yes | Yes | No | No | No | No | No | No |
| AWS::Personalize::Schema | Yes | Yes | No | No | No | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Personalize::Solution | Yes | Yes | No | No | No | No | No | No |
| AWS::Pinpoint::App | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Pinpoint::ApplicationSettings | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Pinpoint::Campaign | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Pinpoint::EmailChannel | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Pinpoint::EmailTemplate | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Pinpoint::EventStream | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Pinpoint::InAppTemplate | Yes | Yes | Yes | No | No | No | No | No |
| AWS::Pinpoint::Segment | Yes | Yes | Yes | No | No | No | No | No |
| AWS::QuickSight::Dashboard | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes |
| AWS::QuickSight::DataSource | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::QuickSight::Template | Yes | Yes | Yes | Yes | Yes | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::QuickSight::Theme | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::RDS::DBCluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBClusterSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBInstance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBProxyEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSubnetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::EventSubscription | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::GlobalCluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::Integration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::OptionGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::RUM::AppMonitor | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterParameterGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSubnetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::EndpointAccess | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Redshift::EndpointAuthorization | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::Redshift::EventSubscription | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::Integration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ScheduledAction | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::ResilienceHub::App | Yes | Yes | Yes | Yes | Yes | Yes | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::ResilienceHub::ResiliencyPolicy | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::ResourceExplorer2::Index | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RoboMaker::RobotApplication | Yes | Yes | No | No | No | No | No | No |
| AWS::RoboMaker::RobotApplicationVersion | Yes | Yes | No | No | No | No | No | No |
| AWS::RoboMaker::SimulationApplication | Yes | Yes | No | No | No | No | No | No |
| AWS::RolesAnywhere::CRL | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RolesAnywhere::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RolesAnywhere::TrustAnchor | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Profiles::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Profiles::ProfileAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::FirewallDomainList | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::Route53Resolver::FirewallRuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::Route53Resolver::FirewallRuleGroupAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| AWS::Route53Resolver::ResolverRule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverRuleAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::AccessGrant | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::AccessGrantsInstance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::AccessGrantsLocation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::AccessPoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::AccountPublicAccessBlock | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::S3::Bucket | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::StorageLens | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::S3::StorageLensGroup | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::S3Express::BucketPolicy | Yes | No | No | No | Yes | No | No | No |
| AWS::S3Express::DirectoryBucket | Yes | No | No | No | Yes | No | No | No |
| AWS::S3Tables::TableBucket | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3Tables::TableBucketPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SES::ConfigurationSet | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SES::ContactList | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SES::DedicatedIpPool | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SES::MailManagerTrafficPolicy | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::SES::ReceiptFilter | Yes | Yes | Yes | Yes | Yes | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::SES::ReceiptRuleSet | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::SES::Template | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SNS::Topic | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SQS::Queue | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SSM::AssociationCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::Document | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::FileData | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::ManagedInstanceInventory | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::PatchCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::ResourceDataSync | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSMContacts::Contact | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::SSMIncidents::ResponsePlan | Yes | Yes | Yes | Yes | Yes | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::AppImageConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| AWS::SageMaker::CodeRepository | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SageMaker::DataQualityJobDefinition | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::SageMaker::Domain | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SageMaker::EndpointConfig | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SageMaker::FeatureGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| AWS::SageMaker::Image | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| AWS::SageMaker::InferenceExperiment | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SageMaker::MlflowTrackingServer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SageMaker::Model | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SageMaker::ModelBiasJobDefinition | Yes | Yes | Yes | Yes | Yes | No | No | No |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::ModelExplainabilityJobDefinition | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::SageMaker::ModelQualityJobDefinition | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::SageMaker::MonitoringSchedule | Yes | Yes | Yes | Yes | Yes | No | No | No |
| AWS::SageMaker::NotebookInstance | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::SageMaker::StudioLifecycleConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SageMaker::UserProfile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SageMaker::Workteam | Yes | Yes | Yes | No | No | No | No | No |
| AWS::SecretsManager::ResourcePolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::RotationSchedule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::Secret | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::SecurityHub::Standard | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProduct | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceCatalog::Portfolio | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceDiscovery::HttpNamespace | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceDiscovery::Instance | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::ServiceDiscovery::PublicDnsNamespace | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ServiceDiscovery::Service | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::ShieldRegional::Protection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Signer::SigningProfile | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::StepFunctions::Activity | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::StepFunctions::StateMachine | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Agreement | Yes | Yes | Yes | Yes | Yes | Yes | No | No |
| AWS::Transfer::Certificate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Connector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Server | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Transfer::Workflow | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFRegional::RateBasedRule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFRegional::Rule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFRegional::RuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFRegional::WebACL | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::IPSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Europe (Ireland) | Europe (Frankfurt) | Europe (London) | Europe (Paris) | Europe (Stockholm) | Europe (Milan) | Europe (Spain) | Europe (Zurich) |
|---|---|---|---|---|---|---|---|---|
| AWS::WAFv2::ManagedRuleSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RegexPatternSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::WebACL | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WorkSpaces::ConnectionAlias | Yes | Yes | Yes | No | No | No | No | No |
| AWS::WorkSpaces::Workspace | Yes | Yes | Yes | No | No | No | No | No |
| AWS::XRay::EncryptionConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

## Asia Pacific Regions

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ACM::Certificate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ACMPCA::CertificateAuthority | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ACMPCA::CertificateAuthorityActivation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::APS::RuleGroupsNamespace | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::AccessAnalyzer::Analyzer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AmazonMQ::Broker | Yes | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Amplify::App | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Amplify::Branch | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ApiGateway::DomainName | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::Method | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::RestApi | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ApiGateway::Stage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ApiGateway::UsagePlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Api | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ApiGatewayV2::Integration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ApiGatewayV2::Stage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::AppConfig::Application | Yes | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppConfig::ConfigurationProfile | Yes | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppConfig::DeploymentStrategy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppConfig::Environment | Yes | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppConfig::Extension | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::AppConfig::ExtensionAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppConfig::HostedConfigurationVersion | Yes | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppFlow::Flow | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppIntegrations::Application | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppIntegrations::DataIntegration | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppIntegrations::EventIntegration | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppMesh::GatewayRoute | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppMesh::Mesh | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::AppMesh::Route | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppMesh::VirtualGateway | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppMesh::VirtualNode | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppMesh::VirtualRouter | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppMesh::VirtualService | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AppRunner::Service | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::AppRunner::VpcConnector | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::AppStream::AppBlockBuilder | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppStream::Application | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::AppStream::DirectoryConfig | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppStream::Fleet | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppStream::Stack | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::AppSync::Api | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::AppSync::ApiCache | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::AppSync::GraphQLApi | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Athena::DataCatalog | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Athena::PreparedStatement | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Athena::WorkGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::AuditManager::Assessment | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Auto Scaling::AutoScalingGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Auto Scaling:: LaunchConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Auto Scaling:: ScalingPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Auto Scaling:: ScheduledAction | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Auto Scaling:: WarmPool | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Back up::BackupPlan | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Back up::BackupSelection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Back up::BackupVault | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Back up::RecoveryPoint | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Backup::ReportPlan | Yes | Yes | Yes | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Backup::RestoreTestingPlan | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::BackupGateway::Hypervisor | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Batch::ComputeEnvironment | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Batch::JobQueue | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Batch::SchedulingPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Bedrock::ApplicationInferenceProfile | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Bedrock::Guardrail | No | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Bedrock::KnowledgeBase | No | Yes | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Bedrock::Prompt | No | Yes | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::BedrockAgentCore::BrowserCustom | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::BedrockAgentCore::CodeInterpreterCustom | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::BedrockAgentCore::Runtime | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::Cassandra::Keyspace | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::CleanRoomsML::TrainingDataset | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Cloud9::EnvironmentEC2 | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CloudFormation::GuardHook | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::CloudFormation::LambdaHook | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CloudFormation::Stack | Yes | No | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::StackSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::CloudTrail::EventDataStore | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CloudTrail::Trail | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::Alarm | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::MetricStream | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CodeArtifact::Domain | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::CodeArtifact::Repository | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::CodeBuild::Project | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::CodeBuild::ReportGroup | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CodeDeploy::Application | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CodeDeploy::DeploymentConfig | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CodeDeploy::DeploymentGroup | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::CodeGuruProfiler::ProfilingGroup | No | No | No | No | No | No | No | No | Yes | Yes | No | No | Yes |
| AWS::CodeGuruReviewer::RepositoryAssociation | No | No | No | No | No | No | No | No | Yes | Yes | No | No | Yes |
| AWS::CodePipeline::Pipeline | Yes | Yes | No | No | Yes | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Cognito::IdentityPool | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Cognito::UserPool | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Cognito::UserPoolClient | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Cognito::UserPoolGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Comprehend::Flywheel | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Config::AggregationAuthorization | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ConfigurationRecorder | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Config::ConformancePack | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Config::ConformancePackCompliance | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Config::ResourceCompliance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Config::StoredQuery | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Connect::Instance | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Connect::PhoneNumber | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Connect::QuickConnect | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Connect::Rule | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Connect::SecurityProfile | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Connect::User | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::CustomerProfiles::Domain | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::CustomerProfiles::ObjectType | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::DMS::Certificate | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::DMS::Endpoint | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DMS::EventSubscription | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DMS::MigrationProject | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DMS::ReplicationInstance | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DMS::ReplicationSubnetGroup | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DMS::ReplicationTask | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::Agent | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationEFS | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::LocationFSxLustre | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::LocationFSxWindows | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::DataSync::LocationHDFS | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::LocationNFS | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::LocationObjectStorage | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::LocationS3 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::LocationSMB | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::DataSync::Task | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Deadline::Fleet | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Deadline::Monitor | No | No | No | No | No | No | No | No | Yes | Yes | No | No | Yes |
| AWS::Deadline::QueueFleetAssociation | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Detective::Graph | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::DynamoDB::Table | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::CapacityReservation | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::CarrierGateway | No | No | No | No | No | No | No | Yes | No | Yes | No | No | Yes |
| AWS::EC2::ClientVpnEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::ClientVpnTargetNetworkAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::CustomerGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::DHCPOptions | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::EC2Fleet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::EIP | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::EIPAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::EgressOnlyInternetGateway | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::FlowLog | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::Host | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAM | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::IPAMPool | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::IPAMPoolCidr | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::IPAMResourceDiscovery | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::IPAMResourceDiscoveryAssociation | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::IPAMScope | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::Instance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::InstanceConnectEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::InternetGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::LaunchTemplate | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::NatGateway | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::NetworkAcl | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::NetworkInsightsAccessScope | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::NetworkInsightsAccessScopeAnalysis | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::NetworkInsightsAnalysis | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::NetworkInsightsPath | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::NetworkInterface | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::PrefixList | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::RouteTable | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SecurityGroupVpcAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SnapshotBlockPublicAccess | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::SpotFleet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::Subnet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetCidrBlock | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::SubnetNetworkAclAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::SubnetRouteTableAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::TrafficMirrorFilter | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::TrafficMirrorSession | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::TrafficMirrorTarget | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::TransitGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::TransitGatewayAttachment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::TransitGatewayConnect | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::TransitGatewayMulticastDomain | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::TransitGatewayRouteTable | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::VPC | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessExclusion | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::VPCBlockPublicAccessOptions | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::VPCEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpointConnectionNotification | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EC2::VPCEndpointService | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCGatewayAttachment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCPeeringConnection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNConnection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNConnectionRoute | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EC2::VPNGateway | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EC2::VerifiedAccessInstance | No | No | Yes | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::EC2::Volume | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::PullThroughCacheRule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ECR::RegistryPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ECR::ReplicationConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECR::Repository | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ECR::RepositoryCreationTemplate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::CapacityProvider | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ECS::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::Service | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::TaskDefinition | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ECS::TaskSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EFS::AccessPoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EFS::FileSystem | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::EKS::Addon | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EKS::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::EKS::FargateProfile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EKS::IdentityProviderConfig | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EMR::SecurityConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EMR::Studio | Yes | No | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EMRContainers::VirtualCluster | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EMRServerless::Application | Yes | Yes | Yes | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::ElasticBeanstalk::Application | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ElasticBeanstalk::ApplicationVersion | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ElasticBeanstalk::Environment | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ElasticLoadBalancing::LoadBalancer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::Listener | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ElasticLoadBalancingV2::LoadBalancer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::TargetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Elasticsearch::Domain | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::EntityResolution::IdMappingWorkflow | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::EntityResolution::MatchingWorkflow | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::EntityResolution::SchemaMapping | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::EventSchemas::Discoverer | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EventSchemas::Registry | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EventSchemas::RegistryPolicy | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::EventSchemas::Schema | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Events::ApiDestination | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Events::Archive | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Events::Connection | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Events::Endpoint | No | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Events::EventBus | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Events::Rule | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::FIS::ExperimentTemplate | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Forecast::Dataset | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Forecast::DatasetGroup | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::FraudDetector::EntityType | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No |
| AWS::FraudDetector::Label | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::FraudDetector::Outcome | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No |
| AWS::FraudDetector::Variable | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No |
| AWS::GameLift::Alias | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::GameLift::Build | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::GameLift::GameSessionQueue | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::GameLift::MatchmakingConfiguration | No | No | No | No | No | No | No | Yes | No | Yes | No | No | Yes |
| AWS::Glue::Classifier | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Glue::Database | Yes | Yes | Yes | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Glue::Job | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Glue::MLTransform | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Glue::Registry | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Grafana::Workspace | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::GreengrassV2::ComponentVersion | No | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::GroundStation::Config | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | No |
| AWS::GroundStation::DataflowEndpointGroup | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | No |
| AWS::GroundStation::MissionProfile | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | No |
| AWS::GuardDuty::Detector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::GuardDuty::Filter | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::GuardDuty::IPSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::GuardDuty::MalwareProtectionPlan | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::GuardDuty::ThreatIntelSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::HealthLake::FHIRDatastore | No | No | No | No | No | Yes | No | No | No | No | No | No | No |
| AWS::IAM::Group | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::IAM::Policy | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::IAM::Role | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::IAM::User | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::IVS::Channel | No | No | No | No | No | Yes | No | Yes | No | No | No | No | Yes |
| AWS::IVS::PlaybackKeyPair | No | No | No | No | No | Yes | No | Yes | No | No | No | No | Yes |
| AWS::IVS::RecordingConfiguration | No | No | No | No | No | Yes | No | Yes | No | No | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ImageBuilder::ContainerRecipe | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ImageBuilder::DistributionConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ImageBuilder::ImagePipeline | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ImageBuilder::ImageRecipe | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ImageBuilder::InfrastructureConfiguration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ImageBuilder::LifecyclePolicy | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::InspectorV2::Activation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::InspectorV2::Filter | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoT::AccountAuditConfiguration | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::Authorizer | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::CACertificate | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::CustomMetric | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::Dimension | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::DomainConfiguration | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::FleetMetric | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::JobTemplate | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::MitigationAction | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::Policy | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::ProvisioningTemplate | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoT::RoleAlias | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::ScheduledAudit | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::SecurityProfile | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoT::ThingGroup | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTAnalytics::Channel | No | No | No | No | No | Yes | No | No | No | Yes | No | No | Yes |
| AWS::IoTAnalytics::Dataset | No | No | No | No | No | Yes | No | No | No | Yes | No | No | Yes |
| AWS::IoTAnalytics::Datastore | No | No | No | No | No | Yes | No | No | No | Yes | No | No | Yes |
| AWS::IoTAnalytics::Pipeline | No | No | No | No | No | Yes | No | No | No | Yes | No | No | Yes |
| AWS::IoTCoreDeviceAdvisor::SuiteDefinition | No | No | No | No | No | No | No | No | No | No | No | No | Yes |
| AWS::IoTEvents::AlarmModel | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoTEvents::DetectorModel | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTEvents::Input | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTSiteWise::Asset | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTSiteWise::AssetModel | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTSiteWise::Dashboard | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTSiteWise::Gateway | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTSiteWise::Portal | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTSiteWise::Project | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTTwinMaker::ComponentType | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTTwinMaker::Entity | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::IoTTwinMaker::Scene | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTTwinMaker::SyncJob | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTTwinMaker::Workspace | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::IoTWireless::FuotaTask | No | No | No | No | No | No | No | No | No | Yes | No | No | Yes |
| AWS::IoTWireless::MulticastGroup | No | No | No | No | No | No | No | No | No | Yes | No | No | Yes |
| AWS::IoTWireless::ServiceProfile | No | No | No | No | No | No | No | No | No | Yes | No | No | Yes |
| AWS::KMS::Alias | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::KMS::Key | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::KafkaConnect::Connector | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::KafkaConnect::CustomPlugin | Yes | Yes | Yes | Yes | No | Yes | No | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Kendra::Index | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::Kinesis::Stream | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Kinesis::StreamConsumer | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::KinesisAnalyticsV2::Application | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::KinesisFirehose::DeliveryStream | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::KinesisVideo::SignalingChannel | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::KinesisVideo::Stream | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Lambda::CodeSigningConfig | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Lambda::Function | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Lex::Bot | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Lex::BotAlias | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Lightsail::Bucket | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Lightsail::Certificate | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Lightsail::Disk | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Lightsail::StaticIp | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Location::APIKey | No | No | No | No | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::Location::GeofenceCollection | No | No | No | Yes | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::Location::Map | No | No | No | Yes | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::Location::PlaceIndex | No | No | No | Yes | No | Yes | No | No | Yes | Yes | No | No | Yes |
| AWS::Location::RouteCalculator | No | No | No | Yes | No | Yes | No | No | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Logs::Destination | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::LookoutVision::Project | No | No | No | No | No | No | No | Yes | No | No | No | No | Yes |
| AWS::M2::Environment | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::MSK::BatchScramSecret | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MSK::Cluster | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MSK::ClusterPolicy | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MSK::Configuration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MSK::ServerlessCluster | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::MSK::VpcConnection | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Macie::Session | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaConnect::FlowEntitlement | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::MediaConnect::FlowSource | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaConnect::FlowVpcInterface | Yes | Yes | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaConnect::Gateway | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaLive::Multiplexprogram | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaPackage::Asset | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaPackage::PackagingConfiguration | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaPackage::PackagingGroup | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaPackageV2::Channel | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::MediaPackageV2::ChannelGroup | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaPackageV2::OriginEndpoint | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaTailor::LiveSource | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MediaTailor::PlaybackConfiguration | No | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::MemoryDB::SubnetGroup | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::NetworkFirewall::Firewall | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::FirewallPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::RuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::NetworkFirewall::TLSInspectionConfiguration | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::VpcEndpointAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Omics::RunGroup | No | No | No | No | No | No | No | Yes | Yes | No | No | No | No |
| AWS::Omics::Workflow | No | No | No | No | No | No | No | Yes | Yes | No | No | No | No |
| AWS::OpenSearch::Domain | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::OpenSearchServerless::Collection | Yes | Yes | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::OpenSearchServerless::SecurityConfig | Yes | Yes | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::OpenSearchServerless::VpcEndpoint | Yes | Yes | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::PCAConnectorAD::Connector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::PCAConnectorAD::DirectoryRegistration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Panorama::Package | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No |
| AWS::Personalize::Dataset | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Personalize::DatasetGroup | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Personalize::Schema | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Personalize::Solution | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Pinpoint::App | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Pinpoint::ApplicationSettings | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Pinpoint::Campaign | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Pinpoint::EmailChannel | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Pinpoint::EmailTemplate | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Pinpoint::EventStream | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Pinpoint::InAppTemplate | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Pinpoint::Segment | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::QuickSight::Dashboard | No | No | Yes | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::QuickSight::DataSource | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::QuickSight::Template | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::QuickSight::Theme | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::RDS::DBCluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBClusterSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::RDS::DBInstance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBProxyEndpoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::RDS::DBSecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSubnetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::EventSubscription | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RDS::GlobalCluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::RDS::Integration | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::RDS::OptionGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::RUM::AppMonitor | No | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Redshift::Cluster | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Redshift::ClusterParameterGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSecurityGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSnapshot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSubnetGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::EndpointAccess | Yes | Yes | Yes | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Redshift::EndpointAuthorization | Yes | Yes | Yes | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::Redshift::EventSubscription | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Redshift::Integration | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Redshift::ScheduledAction | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::ResilienceHub::App | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::ResilienceHub::ResiliencyPolicy | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::ResourceExplorer2::Index | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::RoboMaker::RobotApplication | No | No | No | No | No | No | No | No | Yes | No | No | No | Yes |
| AWS::RoboMaker::RobotApplicationVersion | No | No | No | No | No | No | No | No | Yes | No | No | No | Yes |
| AWS::RoboMaker::SimulationApplication | No | No | No | No | No | No | No | No | Yes | No | No | No | Yes |
| AWS::RolesAnywhere::CRL | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::RolesAnywhere::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::RolesAnywhere::TrustAnchor | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Profiles::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Route53Profiles::ProfileAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Route53Resolver::FirewallDomainList | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Route53Resolver::FirewallRuleGroup | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Route53Resolver::ResolverEndpoint | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverRule | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Route53Resolver::ResolverRuleAssociation | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::S3::AccessGrant | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::S3::AccessGrantsInstance | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::S3::AccessGrantsLocation | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::S3::AccessPoint | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::S3::AccountPublicAccessBlock | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::S3::Bucket | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::S3::StorageLens | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::S3::StorageLensGroup | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::S3Express::BucketPolicy | No | No | No | No | No | Yes | No | No | No | No | No | No | Yes |
| AWS::S3Express::DirectoryBucket | No | No | No | No | No | Yes | No | No | No | No | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::S3Tables::TableBucket | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::S3Tables::TableBucketPolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::SES::ConfigurationSet | No | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SES::ContactList | No | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SES::DedicatedIpPool | No | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SES::MailManagerTrafficPolicy | No | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SES::ReceiptFilter | No | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SES::ReceiptRuleSet | No | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SES::Template | No | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SNS::Topic | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SQS::Queue | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::SSM::AssociationCompliance | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::Document | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SSM::FileData | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::ManagedInstanceInventory | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::PatchCompliance | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSM::ResourceDataSync | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SSMContacts::Contact | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::SSMIncidents::ResponsePlan | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::AppImageConfig | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::CodeRepository | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::DataQualityJobDefinition | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::Domain | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::EndpointConfig | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::FeatureGroup | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::Image | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::InferenceExperiment | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::MlflowTrackingServer | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::Model | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::ModelBiasJobDefinition | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::ModelExplainabilityJobDefinition | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::ModelQualityJobDefinition | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::MonitoringSchedule | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::NotebookInstance | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | Yes | No | No | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::SageMaker::StudioLifecycleConfig | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::UserProfile | Yes | No | Yes | No | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::SageMaker::Workteam | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::SecretsManager::ResourcePolicy | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::RotationSchedule | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::Secret | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::SecurityHub::Standard | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProduct | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ServiceCatalog::Portfolio | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ServiceDiscovery::HttpNamespace | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ServiceDiscovery::Instance | Yes | No | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ServiceDiscovery::PublicDnsNamespace | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::ServiceDiscovery::Service | Yes | No | No | Yes | No | Yes | No | Yes | Yes | Yes | No | No | Yes |
| AWS::ShieldRegional::Protection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | Yes | Yes |
| AWS::Signer::SigningProfile | Yes | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::Step Functions::Activity | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Step Functions::StateMachine | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Transfer::Agreement | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Transfer::Certificate | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Transfer::Connector | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Transfer::Profile | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Transfer::Server | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::Transfer::Workflow | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::WAFRegional::RateBasedRule | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::WAFRegional::Rule | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::WAFRegional::RuleGroup | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::WAFRegional::WebACL | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes |
| AWS::WAFv2::IPSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::ManagedRuleSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RegexPatternSet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RuleGroup | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WAFv2::WebACL | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| AWS::WorkSpaces::ConnectionAlias | No | No | No | No | No | No | No | Yes | Yes | Yes | No | No | Yes |
| AWS::WorkSpaces::Workspace | No | No | No | No | No | Yes | No | Yes | Yes | Yes | No | No | Yes |

| Resource type | Asia Pacific (Hong Kong) | Asia Pacific (Hyderabad) | Asia Pacific (Jakarta) | Asia Pacific (Malaysia) | Asia Pacific (Melbourne) | Asia Pacific (Mumbai) | Asia Pacific (Osaka) | Asia Pacific (Seoul) | Asia Pacific (Singapore) | Asia Pacific (Sydney) | Asia Pacific (Taipei) | Asia Pacific (Thailand) | Asia Pacific (Tokyo) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AWS::XRay::EncryptionConfig | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

## China Regions

| Resource type | China (Beijing) | China (Ningxia) |
|---|---|---|
| AWS::ACM::Certificate | Yes | Yes |
| AWS::AmazonMQ::Broker | Yes | Yes |
| AWS::ApiGateway::DomainName | Yes | Yes |
| AWS::ApiGateway::Method | Yes | Yes |
| AWS::ApiGateway::RestApi | Yes | Yes |
| AWS::ApiGateway::Stage | Yes | Yes |
| AWS::ApiGateway::UsagePlan | Yes | Yes |
| AWS::ApiGatewayV2::Api | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::ApiGatewayV2::Integration | Yes | Yes |
| AWS::ApiGatewayV2::Stage | Yes | Yes |
| AWS::AppConfig::Application | Yes | Yes |
| AWS::AppConfig::ConfigurationProfile | Yes | Yes |
| AWS::AppConfig::DeploymentStrategy | Yes | Yes |
| AWS::AppConfig::Environment | Yes | Yes |
| AWS::AppConfig::Extension | Yes | Yes |
| AWS::AppConfig::ExtensionAssociation | Yes | Yes |
| AWS::AppConfig::HostedConfigurationVersion | Yes | Yes |
| AWS::AppSync::Api | Yes | Yes |
| AWS::AppSync::ApiCache | Yes | Yes |
| AWS::AppSync::GraphQLApi | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::Athena::DataCatalog | Yes | Yes |
| AWS::Athena::PreparedStatement | Yes | Yes |
| AWS::Athena::WorkGroup | Yes | Yes |
| AWS::AutoScaling::AutoScalingGroup | Yes | Yes |
| AWS::AutoScaling::LaunchConfiguration | Yes | Yes |
| AWS::AutoScaling::ScalingPolicy | Yes | Yes |
| AWS::AutoScaling::ScheduledAction | Yes | Yes |
| AWS::AutoScaling::WarmPool | Yes | Yes |
| AWS::Backup::BackupPlan | Yes | Yes |
| AWS::Backup::BackupSelection | Yes | Yes |
| AWS::Backup::BackupVault | Yes | Yes |
| AWS::Backup::RecoveryPoint | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::Batch::ComputeEnvironment | Yes | Yes |
| AWS::Batch::JobQueue | Yes | Yes |
| AWS::Batch::SchedulingPolicy | Yes | Yes |
| AWS::Cassandra::Keyspace | Yes | Yes |
| AWS::CloudFormation::Stack | Yes | Yes |
| AWS::CloudFormation::StackSet | Yes | Yes |
| AWS::CloudFront::PublicKey | Yes | No |
| AWS::CloudTrail::Trail | Yes | Yes |
| AWS::CloudWatch::Alarm | Yes | Yes |
| AWS::CloudWatch::MetricStream | Yes | Yes |
| AWS::CodeBuild::Project | Yes | Yes |
| AWS::CodeBuild::ReportGroup | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::Cognito::IdentityPool | Yes | No |
| AWS::Config::AggregationAuthorization | Yes | Yes |
| AWS::Config::ConfigurationRecorder | Yes | Yes |
| AWS::Config::ResourceCompliance | Yes | Yes |
| AWS::Config::StoredQuery | Yes | Yes |
| AWS::DMS::Certificate | Yes | Yes |
| AWS::DMS::Endpoint | Yes | Yes |
| AWS::DMS::EventSubscription | Yes | Yes |
| AWS::DMS::ReplicationInstance | Yes | Yes |
| AWS::DMS::ReplicationSubnetGroup | Yes | Yes |
| AWS::DMS::ReplicationTask | Yes | Yes |
| AWS::DataSync::Agent | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::DataSync::LocationEFS | Yes | Yes |
| AWS::DataSync::LocationHDFS | Yes | Yes |
| AWS::DataSync::LocationNFS | Yes | Yes |
| AWS::DataSync::LocationObjectStorage | Yes | Yes |
| AWS::DataSync::LocationS3 | Yes | Yes |
| AWS::DataSync::LocationSMB | Yes | Yes |
| AWS::DataSync::Task | Yes | Yes |
| AWS::DynamoDB::Table | Yes | Yes |
| AWS::EC2::CapacityReservation | Yes | Yes |
| AWS::EC2::DHCPOptions | Yes | Yes |
| AWS::EC2::EC2Fleet | Yes | Yes |
| AWS::EC2::EIP | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::EC2::EIPAssociation | Yes | Yes |
| AWS::EC2::FlowLog | Yes | Yes |
| AWS::EC2::Host | Yes | Yes |
| AWS::EC2::Instance | Yes | Yes |
| AWS::EC2::InternetGateway | Yes | Yes |
| AWS::EC2::LaunchTemplate | Yes | Yes |
| AWS::EC2::NatGateway | Yes | Yes |
| AWS::EC2::NetworkAcl | Yes | Yes |
| AWS::EC2::NetworkInterface | Yes | Yes |
| AWS::EC2::PrefixList | Yes | Yes |
| AWS::EC2::RouteTable | Yes | Yes |
| AWS::EC2::SecurityGroup | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::EC2::SecurityGroupVpcAssociation | Yes | Yes |
| AWS::EC2::SnapshotBlockPublicAccess | Yes | Yes |
| AWS::EC2::SpotFleet | Yes | Yes |
| AWS::EC2::Subnet | Yes | Yes |
| AWS::EC2::SubnetCidrBlock | Yes | No |
| AWS::EC2::SubnetNetworkAclAssociation | Yes | Yes |
| AWS::EC2::SubnetRouteTableAssociation | Yes | Yes |
| AWS::EC2::TrafficMirrorFilter | Yes | Yes |
| AWS::EC2::TrafficMirrorSession | Yes | Yes |
| AWS::EC2::TrafficMirrorTarget | Yes | Yes |
| AWS::EC2::TransitGateway | Yes | Yes |
| AWS::EC2::TransitGatewayAttachment | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::EC2::TransitGatewayConnect | Yes | Yes |
| AWS::EC2::TransitGatewayMulticastDomain | Yes | Yes |
| AWS::EC2::TransitGatewayRouteTable | Yes | Yes |
| AWS::EC2::VPC | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessExclusion | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessOptions | Yes | Yes |
| AWS::EC2::VPCEndpoint | Yes | Yes |
| AWS::EC2::VPCEndpointConnectionNotification | Yes | Yes |
| AWS::EC2::VPCEndpointService | Yes | Yes |
| AWS::EC2::VPCGatewayAttachment | Yes | Yes |
| AWS::EC2::VPCPeeringConnection | Yes | Yes |
| AWS::EC2::VPNGateway | Yes | No |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::EC2::Volume | Yes | Yes |
| AWS::ECR::ReplicationConfiguration | Yes | Yes |
| AWS::ECR::Repository | Yes | Yes |
| AWS::ECS::CapacityProvider | Yes | Yes |
| AWS::ECS::Cluster | Yes | Yes |
| AWS::ECS::Service | Yes | Yes |
| AWS::ECS::TaskDefinition | Yes | Yes |
| AWS::ECS::TaskSet | Yes | Yes |
| AWS::EFS::AccessPoint | Yes | Yes |
| AWS::EFS::FileSystem | Yes | Yes |
| AWS::EKS::Addon | Yes | Yes |
| AWS::EKS::Cluster | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
|---|---|---|
| AWS::EKS::FargateProfile | Yes | Yes |
| AWS::EKS::IdentityProviderConfig | Yes | Yes |
| AWS::EMR::SecurityConfiguration | Yes | Yes |
| AWS::EMR::Studio | Yes | Yes |
| AWS::EMRContainers::VirtualCluster | Yes | Yes |
| AWS::EMRServerless::Application | Yes | Yes |
| AWS::ElasticBeanstalk::Application | Yes | Yes |
| AWS::ElasticBeanstalk::ApplicationVersion | Yes | Yes |
| AWS::ElasticBeanstalk::Environment | Yes | Yes |
| AWS::ElasticLoadBalancing::LoadBalancer | Yes | Yes |
| AWS::ElasticLoadBalancingV2::Listener | Yes | Yes |
| AWS::ElasticLoadBalancingV2::LoadBalancer | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::ElasticLoadBalancingV2::TargetGroup | Yes | Yes |
| AWS::Elasticsearch::Domain | Yes | Yes |
| AWS::Events::Archive | Yes | Yes |
| AWS::Events::EventBus | Yes | Yes |
| AWS::Events::Rule | Yes | Yes |
| AWS::GameLift::Alias | Yes | Yes |
| AWS::GameLift::GameSessionQueue | Yes | Yes |
| AWS::GameLift::MatchmakingConfiguration | Yes | Yes |
| AWS::Glue::Classifier | Yes | Yes |
| AWS::Glue::Job | Yes | Yes |
| AWS::Glue::MLTransform | Yes | No |
| AWS::Glue::Registry | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::GreengrassV2::ComponentVersion | Yes | No |
| AWS::GuardDuty::Filter | Yes | Yes |
| AWS::GuardDuty::ThreatIntelSet | Yes | Yes |
| AWS::IAM::Group | Yes | Yes |
| AWS::IAM::InstanceProfile | Yes | No |
| AWS::IAM::OIDCProvider | Yes | No |
| AWS::IAM::Policy | Yes | Yes |
| AWS::IAM::Role | Yes | Yes |
| AWS::IAM::SAMLProvider | Yes | No |
| AWS::IAM::ServerCertificate | Yes | No |
| AWS::IAM::User | Yes | Yes |
| AWS::ImageBuilder::ContainerRecipe | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::ImageBuilder::DistributionConfiguration | Yes | Yes |
| AWS::ImageBuilder::ImagePipeline | Yes | Yes |
| AWS::ImageBuilder::ImageRecipe | Yes | Yes |
| AWS::ImageBuilder::InfrastructureConfiguration | Yes | Yes |
| AWS::InspectorV2::Activation | Yes | Yes |
| AWS::IoT::AccountAuditConfiguration | Yes | Yes |
| AWS::IoT::Authorizer | Yes | Yes |
| AWS::IoT::CACertificate | Yes | Yes |
| AWS::IoT::CustomMetric | Yes | Yes |
| AWS::IoT::Dimension | Yes | Yes |
| AWS::IoT::DomainConfiguration | Yes | Yes |
| AWS::IoT::FleetMetric | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::IoT::JobTemplate | Yes | Yes |
| AWS::IoT::MitigationAction | Yes | Yes |
| AWS::IoT::Policy | Yes | Yes |
| AWS::IoT::ProvisioningTemplate | Yes | Yes |
| AWS::IoT::RoleAlias | Yes | Yes |
| AWS::IoT::ScheduledAudit | Yes | Yes |
| AWS::IoT::SecurityProfile | Yes | Yes |
| AWS::IoT::ThingGroup | Yes | Yes |
| AWS::IoTAnalytics::Channel | Yes | No |
| AWS::IoTAnalytics::Dataset | Yes | No |
| AWS::IoTAnalytics::Datastore | Yes | No |
| AWS::IoTAnalytics::Pipeline | Yes | No |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::IoTEvents::AlarmModel | Yes | No |
| AWS::IoTEvents::DetectorModel | Yes | No |
| AWS::IoTEvents::Input | Yes | No |
| AWS::IoTSiteWise::Asset | Yes | No |
| AWS::IoTSiteWise::AssetModel | Yes | No |
| AWS::IoTSiteWise::Dashboard | Yes | No |
| AWS::IoTSiteWise::Gateway | Yes | No |
| AWS::IoTSiteWise::Portal | Yes | No |
| AWS::IoTSiteWise::Project | Yes | No |
| AWS::KMS::Alias | Yes | Yes |
| AWS::KMS::Key | Yes | Yes |
| AWS::Kinesis::Stream | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::Kinesis::StreamConsumer | Yes | Yes |
| AWS::KinesisAnalyticsV2::Application | Yes | Yes |
| AWS::KinesisFirehose::DeliveryStream | Yes | Yes |
| AWS::Lambda::Function | Yes | No |
| AWS::Logs::Destination | Yes | Yes |
| AWS::MSK::BatchScramSecret | Yes | Yes |
| AWS::MSK::Cluster | Yes | Yes |
| AWS::MSK::ClusterPolicy | Yes | Yes |
| AWS::MSK::Configuration | Yes | Yes |
| AWS::MSK::VpcConnection | Yes | Yes |
| AWS::NetworkFirewall::Firewall | Yes | Yes |
| AWS::NetworkFirewall::FirewallPolicy | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::NetworkFirewall::RuleGroup | Yes | Yes |
| AWS::NetworkFirewall::TLSInspectionConfiguration | Yes | Yes |
| AWS::NetworkFirewall::VpcEndpointAssociation | Yes | Yes |
| AWS::OpenSearch::Domain | Yes | Yes |
| AWS::Personalize::Dataset | Yes | No |
| AWS::Personalize::DatasetGroup | Yes | No |
| AWS::Personalize::Schema | Yes | No |
| AWS::Personalize::Solution | Yes | No |
| AWS::QuickSight::Dashboard | Yes | No |
| AWS::RDS::DBCluster | No | Yes |
| AWS::RDS::DBClusterSnapshot | Yes | Yes |
| AWS::RDS::DBInstance | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::RDS::DBProxyEndpoint | Yes | Yes |
| AWS::RDS::DBSecurityGroup | Yes | Yes |
| AWS::RDS::DBSnapshot | Yes | Yes |
| AWS::RDS::DBSubnetGroup | Yes | Yes |
| AWS::RDS::EventSubscription | Yes | Yes |
| AWS::RDS::Integration | Yes | Yes |
| AWS::RDS::OptionGroup | Yes | Yes |
| AWS::Redshift::Cluster | Yes | Yes |
| AWS::Redshift::ClusterParameterGroup | Yes | Yes |
| AWS::Redshift::ClusterSecurityGroup | Yes | Yes |
| AWS::Redshift::ClusterSnapshot | Yes | Yes |
| AWS::Redshift::ClusterSubnetGroup | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
|---|---|---|
| AWS::Redshift::EventSubscription | Yes | Yes |
| AWS::Redshift::Integration | Yes | Yes |
| AWS::RolesAnywhere::CRL | Yes | Yes |
| AWS::RolesAnywhere::Profile | Yes | Yes |
| AWS::RolesAnywhere::TrustAnchor | Yes | Yes |
| AWS::Route53Profiles::Profile | Yes | Yes |
| AWS::Route53Profiles::ProfileAssociation | Yes | Yes |
| AWS::Route53Resolver::FirewallDomainList | Yes | Yes |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | Yes | Yes |
| AWS::Route53Resolver::ResolverEndpoint | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
|---|---|---|
| AWS::Route53Resolver::ResolverRule | Yes | Yes |
| AWS::Route53Resolver::ResolverRuleAssociation | Yes | Yes |
| AWS::S3::AccessGrant | Yes | Yes |
| AWS::S3::AccessGrantsInstance | Yes | Yes |
| AWS::S3::AccessGrantsLocation | Yes | Yes |
| AWS::S3::AccessPoint | Yes | Yes |
| AWS::S3::AccountPublicAccessBlock | Yes | Yes |
| AWS::S3::Bucket | Yes | Yes |
| AWS::S3::StorageLensGroup | Yes | Yes |
| AWS::SES::ConfigurationSet | No | Yes |
| AWS::SES::ContactList | No | Yes |
| AWS::SES::Template | No | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::SNS::Topic | Yes | Yes |
| AWS::SQS::Queue | Yes | Yes |
| AWS::SSM::AssociationCompliance | Yes | Yes |
| AWS::SSM::Document | Yes | Yes |
| AWS::SSM::FileData | Yes | Yes |
| AWS::SSM::ManagedInstanceInventory | Yes | Yes |
| AWS::SSM::PatchCompliance | Yes | Yes |
| AWS::SSM::ResourceDataSync | Yes | Yes |
| AWS::SageMaker::AppImageConfig | Yes | Yes |
| AWS::SageMaker::CodeRepository | Yes | Yes |
| AWS::SageMaker::Domain | Yes | Yes |
| AWS::SageMaker::EndpointConfig | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::SageMaker::FeatureGroup | Yes | Yes |
| AWS::SageMaker::Image | Yes | Yes |
| AWS::SageMaker::Model | Yes | Yes |
| AWS::SageMaker::MonitoringSchedule | Yes | Yes |
| AWS::SageMaker::NotebookInstance | Yes | Yes |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | Yes | Yes |
| AWS::SageMaker::StudioLifecycleConfig | Yes | Yes |
| AWS::SageMaker::UserProfile | Yes | Yes |
| AWS::SecretsManager::ResourcePolicy | Yes | Yes |
| AWS::SecretsManager::RotationSchedule | Yes | Yes |
| AWS::SecretsManager::Secret | Yes | Yes |
| AWS::SecurityHub::Standard | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::ServiceCatalog::CloudFormationProduct | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | Yes | Yes |
| AWS::ServiceCatalog::Portfolio | Yes | Yes |
| AWS::ServiceDiscovery::HttpNamespace | Yes | Yes |
| AWS::ServiceDiscovery::Instance | Yes | Yes |
| AWS::ServiceDiscovery::PublicDnsNamespace | Yes | Yes |
| AWS::ServiceDiscovery::Service | Yes | Yes |
| AWS::StepFunctions::Activity | Yes | No |
| AWS::StepFunctions::StateMachine | Yes | Yes |
| AWS::Transfer::Agreement | Yes | Yes |
| AWS::Transfer::Certificate | Yes | Yes |
| AWS::Transfer::Connector | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
| --- | --- | --- |
| AWS::Transfer::Profile | Yes | Yes |
| AWS::Transfer::Server | Yes | Yes |
| AWS::Transfer::Workflow | Yes | Yes |
| AWS::WAFRegional::RateBasedRule | Yes | Yes |
| AWS::WAFRegional::Rule | Yes | Yes |
| AWS::WAFRegional::RuleGroup | Yes | Yes |
| AWS::WAFRegional::WebACL | Yes | Yes |
| AWS::WAFv2::IPSet | Yes | Yes |
| AWS::WAFv2::ManagedRuleSet | Yes | Yes |
| AWS::WAFv2::RegexPatternSet | Yes | Yes |
| AWS::WAFv2::RuleGroup | Yes | Yes |
| AWS::WAFv2::WebACL | Yes | Yes |

| Resource type | China (Beijing) | China (Ningxia) |
|---|---|---|
| AWS::WorkSpaces::Workspace | No | Yes |

## Africa and Middle East Regions

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::ACM::Certificate | Yes | Yes | Yes | Yes |
| AWS::ACMPCA::CertificateAuthority | Yes | Yes | Yes | Yes |
| AWS::ACMPCA::CertificateAuthorityActivation | Yes | Yes | Yes | Yes |
| AWS::APS::RuleGroupsNamespace | Yes | No | Yes | Yes |
| AWS::AccessAnalyzer::Analyzer | Yes | Yes | Yes | Yes |
| AWS::AmazonMQ::Broker | Yes | No | Yes | Yes |
| AWS::Amplify::App | No | No | Yes | No |
| AWS::Amplify::Branch | No | No | Yes | No |
| AWS::ApiGateway::DomainName | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::ApiGateway::Method | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::RestApi | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::Stage | Yes | Yes | Yes | Yes |
| AWS::ApiGateway::UsagePlan | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Api | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Integration | Yes | Yes | Yes | Yes |
| AWS::ApiGatewayV2::Stage | Yes | Yes | Yes | Yes |
| AWS::AppConfig::Application | Yes | Yes | Yes | No |
| AWS::AppConfig::ConfigurationProfile | Yes | Yes | Yes | No |
| AWS::AppConfig::DeploymentStrategy | Yes | Yes | Yes | Yes |
| AWS::AppConfig::Environment | Yes | Yes | Yes | No |
| AWS::AppConfig::Extension | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::AppConfig::ExtensionAssociation | Yes | Yes | Yes | Yes |
| AWS::AppConfig::HostedConfigurationVersion | Yes | Yes | Yes | No |
| AWS::AppFlow::Flow | Yes | No | No | No |
| AWS::AppIntegrations::Application | Yes | No | No | No |
| AWS::AppIntegrations::DataIntegration | Yes | No | No | No |
| AWS::AppIntegrations::EventIntegration | Yes | No | No | No |
| AWS::AppMesh::GatewayRoute | Yes | Yes | Yes | No |
| AWS::AppMesh::Mesh | Yes | Yes | Yes | No |
| AWS::AppMesh::Route | Yes | Yes | Yes | No |
| AWS::AppMesh::VirtualGateway | Yes | Yes | Yes | No |
| AWS::AppMesh::VirtualNode | Yes | Yes | Yes | No |
| AWS::AppMesh::VirtualRouter | Yes | Yes | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::AppMesh::VirtualService | Yes | Yes | Yes | No |
| AWS::AppSync::Api | Yes | Yes | Yes | Yes |
| AWS::AppSync::ApiCache | Yes | Yes | Yes | Yes |
| AWS::AppSync::GraphQLApi | Yes | Yes | Yes | Yes |
| AWS::Athena::DataCatalog | Yes | Yes | Yes | Yes |
| AWS::Athena::PreparedStatement | Yes | Yes | Yes | Yes |
| AWS::Athena::WorkGroup | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::AutoScalingGroup | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::LaunchConfiguration | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::ScalingPolicy | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::ScheduledAction | Yes | Yes | Yes | Yes |
| AWS::AutoScaling::WarmPool | Yes | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::Backup::BackupPlan | Yes | Yes | Yes | Yes |
| AWS::Backup::BackupSelection | Yes | Yes | Yes | Yes |
| AWS::Backup::BackupVault | Yes | Yes | Yes | Yes |
| AWS::Backup::RecoveryPoint | Yes | Yes | Yes | Yes |
| AWS::Backup::ReportPlan | Yes | No | Yes | Yes |
| AWS::Backup::RestoreTestingPlan | Yes | No | Yes | Yes |
| AWS::BackupGateway::Hypervisor | Yes | No | Yes | No |
| AWS::Batch::ComputeEnvironment | Yes | No | Yes | Yes |
| AWS::Batch::JobQueue | Yes | No | Yes | Yes |
| AWS::Batch::SchedulingPolicy | Yes | Yes | Yes | Yes |
| AWS::Bedrock::Guardrail | No | No | No | Yes |
| AWS::Cassandra::Keyspace | No | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::Cloud9::EnvironmentEC2 | Yes | No | Yes | No |
| AWS::CloudFormation::GuardHook | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::LambdaHook | Yes | Yes | Yes | Yes |
| AWS::CloudFormation::Stack | Yes | No | Yes | No |
| AWS::CloudFormation::StackSet | Yes | Yes | Yes | Yes |
| AWS::CloudTrail::EventDataStore | Yes | Yes | Yes | Yes |
| AWS::CloudTrail::Trail | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::Alarm | Yes | Yes | Yes | Yes |
| AWS::CloudWatch::MetricStream | Yes | Yes | Yes | Yes |
| AWS::CodeBuild::Project | Yes | Yes | Yes | Yes |
| AWS::CodeBuild::ReportGroup | Yes | Yes | Yes | Yes |
| AWS::CodeDeploy::Application | Yes | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::CodeDeploy::DeploymentConfig | Yes | No | Yes | No |
| AWS::CodeDeploy::DeploymentGroup | Yes | No | Yes | No |
| AWS::CodePipeline::Pipeline | No | Yes | No | Yes |
| AWS::Cognito::IdentityPool | Yes | Yes | Yes | Yes |
| AWS::Cognito::UserPool | Yes | Yes | Yes | Yes |
| AWS::Cognito::UserPoolClient | Yes | Yes | Yes | Yes |
| AWS::Cognito::UserPoolGroup | Yes | Yes | Yes | Yes |
| AWS::Config::AggregationAuthorization | Yes | Yes | Yes | Yes |
| AWS::Config::ConfigurationRecorder | Yes | Yes | Yes | Yes |
| AWS::Config::ConformancePack | Yes | Yes | Yes | Yes |
| AWS::Config::ConformancePackCompliance | Yes | Yes | Yes | Yes |
| AWS::Config::ResourceCompliance | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::Config::StoredQuery | Yes | Yes | Yes | Yes |
| AWS::Connect::Instance | Yes | No | No | No |
| AWS::Connect::PhoneNumber | Yes | No | No | No |
| AWS::Connect::QuickConnect | Yes | No | No | No |
| AWS::Connect::Rule | Yes | No | No | No |
| AWS::Connect::SecurityProfile | Yes | No | No | No |
| AWS::Connect::User | Yes | No | No | No |
| AWS::CustomerProfiles::Domain | Yes | No | No | No |
| AWS::CustomerProfiles::ObjectType | Yes | No | No | No |
| AWS::DMS::Certificate | Yes | No | Yes | No |
| AWS::DMS::Endpoint | Yes | No | Yes | No |
| AWS::DMS::EventSubscription | Yes | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::DMS::MigrationProject | Yes | Yes | Yes | Yes |
| AWS::DMS::ReplicationInstance | Yes | No | Yes | No |
| AWS::DMS::ReplicationSubnetGroup | Yes | No | Yes | No |
| AWS::DMS::ReplicationTask | Yes | No | Yes | No |
| AWS::DataSync::Agent | Yes | Yes | Yes | Yes |
| AWS::DataSync::LocationEFS | Yes | No | Yes | Yes |
| AWS::DataSync::LocationFSxLustre | Yes | No | Yes | Yes |
| AWS::DataSync::LocationFSxWindows | Yes | No | Yes | No |
| AWS::DataSync::LocationHDFS | Yes | No | Yes | Yes |
| AWS::DataSync::LocationNFS | Yes | No | Yes | Yes |
| AWS::DataSync::LocationObjectStorage | Yes | No | Yes | Yes |
| AWS::DataSync::LocationS3 | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::DataSync::LocationSMB | Yes | No | Yes | Yes |
| AWS::DataSync::Task | Yes | Yes | Yes | Yes |
| AWS::Detective::Graph | Yes | Yes | Yes | No |
| AWS::DynamoDB::Table | Yes | Yes | Yes | Yes |
| AWS::EC2::CapacityReservation | Yes | Yes | Yes | Yes |
| AWS::EC2::ClientVpnEndpoint | Yes | No | Yes | Yes |
| AWS::EC2::ClientVpnTargetNetworkAssociation | Yes | Yes | Yes | Yes |
| AWS::EC2::CustomerGateway | Yes | Yes | Yes | Yes |
| AWS::EC2::DHCPOptions | Yes | Yes | Yes | Yes |
| AWS::EC2::EC2Fleet | Yes | No | Yes | Yes |
| AWS::EC2::EIP | Yes | Yes | Yes | Yes |
| AWS::EC2::EIPAssociation | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::EC2::EgressOnlyInternetGateway | Yes | No | Yes | Yes |
| AWS::EC2::FlowLog | Yes | Yes | Yes | Yes |
| AWS::EC2::Host | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAM | Yes | No | Yes | Yes |
| AWS::EC2::IPAMPool | Yes | No | Yes | Yes |
| AWS::EC2::IPAMPoolCidr | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMResourceDiscovery | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMResourceDiscoveryAssociation | Yes | Yes | Yes | Yes |
| AWS::EC2::IPAMScope | Yes | No | Yes | Yes |
| AWS::EC2::Instance | Yes | Yes | Yes | Yes |
| AWS::EC2::InstanceConnectEndpoint | Yes | Yes | Yes | Yes |
| AWS::EC2::InternetGateway | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::EC2::LaunchTemplate | Yes | No | Yes | No |
| AWS::EC2::NatGateway | Yes | No | Yes | Yes |
| AWS::EC2::NetworkAcl | Yes | Yes | Yes | Yes |
| AWS::EC2::NetworkInsightsAccessScope | Yes | No | Yes | Yes |
| AWS::EC2::NetworkI nsightsAccessScopeAnalysis | Yes | No | Yes | Yes |
| AWS::EC2::NetworkInsightsAnalysis | Yes | No | Yes | No |
| AWS::EC2::NetworkInsightsPath | Yes | No | Yes | Yes |
| AWS::EC2::NetworkInterface | Yes | Yes | Yes | Yes |
| AWS::EC2::PrefixList | Yes | Yes | Yes | Yes |
| AWS::EC2::RouteTable | Yes | Yes | Yes | Yes |
| AWS::EC2::SecurityGroup | Yes | Yes | Yes | Yes |
| AWS::EC2::SecurityGroupVpcAssociation | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::EC2::SnapshotBlockPublicAccess | Yes | Yes | Yes | Yes |
| AWS::EC2::SpotFleet | Yes | Yes | Yes | Yes |
| AWS::EC2::Subnet | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetCidrBlock | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetNetworkAclAssociation | Yes | Yes | Yes | Yes |
| AWS::EC2::SubnetRouteTableAssociation | Yes | Yes | Yes | Yes |
| AWS::EC2::TrafficMirrorFilter | Yes | Yes | Yes | Yes |
| AWS::EC2::TrafficMirrorSession | Yes | No | Yes | Yes |
| AWS::EC2::TrafficMirrorTarget | Yes | No | Yes | Yes |
| AWS::EC2::TransitGateway | Yes | Yes | Yes | Yes |
| AWS::EC2::TransitGatewayAttachment | Yes | No | Yes | Yes |
| AWS::EC2::TransitGatewayConnect | Yes | No | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::EC2::TransitGatewayMulticastDomain | Yes | Yes | Yes | Yes |
| AWS::EC2::TransitGatewayRouteTable | Yes | No | Yes | Yes |
| AWS::EC2::VPC | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessExclusion | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessOptions | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpoint | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpointConnectionNotification | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCEndpointService | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCGatewayAttachment | Yes | Yes | Yes | Yes |
| AWS::EC2::VPCPeeringConnection | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNConnection | Yes | Yes | Yes | Yes |
| AWS::EC2::VPNConnectionRoute | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::EC2::VPNGateway | Yes | Yes | Yes | Yes |
| AWS::EC2::VerifiedAccessInstance | No | Yes | No | No |
| AWS::EC2::Volume | Yes | Yes | Yes | Yes |
| AWS::ECR::PullThroughCacheRule | Yes | Yes | Yes | Yes |
| AWS::ECR::RegistryPolicy | Yes | Yes | Yes | Yes |
| AWS::ECR::ReplicationConfiguration | Yes | Yes | Yes | Yes |
| AWS::ECR::Repository | Yes | Yes | Yes | Yes |
| AWS::ECR::RepositoryCreationTemplate | Yes | Yes | Yes | Yes |
| AWS::ECS::CapacityProvider | Yes | Yes | Yes | Yes |
| AWS::ECS::Cluster | Yes | Yes | Yes | Yes |
| AWS::ECS::Service | Yes | Yes | Yes | Yes |
| AWS::ECS::TaskDefinition | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::ECS::TaskSet | Yes | No | Yes | Yes |
| AWS::EFS::AccessPoint | Yes | Yes | Yes | Yes |
| AWS::EFS::FileSystem | Yes | Yes | Yes | Yes |
| AWS::EKS::Addon | Yes | No | Yes | Yes |
| AWS::EKS::Cluster | Yes | Yes | Yes | Yes |
| AWS::EKS::FargateProfile | Yes | Yes | Yes | Yes |
| AWS::EKS::IdentityProviderConfig | Yes | No | Yes | Yes |
| AWS::EMR::SecurityConfiguration | Yes | Yes | Yes | Yes |
| AWS::EMR::Studio | Yes | Yes | Yes | Yes |
| AWS::EMRContainers::VirtualCluster | Yes | Yes | Yes | Yes |
| AWS::EMRServerless::Application | Yes | No | Yes | Yes |
| AWS::ElasticBeanstalk::Application | Yes | No | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::ElasticBeanstalk::ApplicationVersion | Yes | No | Yes | Yes |
| AWS::ElasticBeanstalk::Environment | Yes | No | Yes | Yes |
| AWS::ElasticLoadBalancing::LoadBalancer | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::Listener | Yes | No | Yes | Yes |
| AWS::ElasticLoadBalancingV2::LoadBalancer | Yes | Yes | Yes | Yes |
| AWS::ElasticLoadBalancingV2::TargetGroup | Yes | Yes | Yes | Yes |
| AWS::Elasticsearch::Domain | Yes | Yes | Yes | Yes |
| AWS::EntityResolution::IdMappingWorkflow | Yes | No | No | No |
| AWS::EntityResolution::MatchingWorkflow | Yes | No | No | No |
| AWS::EntityResolution::SchemaMapping | Yes | No | No | No |
| AWS::EventSchemas::Discoverer | Yes | No | Yes | Yes |
| AWS::EventSchemas::Registry | Yes | No | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::EventSchemas::RegistryPolicy | Yes | No | Yes | Yes |
| AWS::EventSchemas::Schema | Yes | No | Yes | Yes |
| AWS::Events::ApiDestination | Yes | No | Yes | Yes |
| AWS::Events::Archive | Yes | No | Yes | Yes |
| AWS::Events::Connection | Yes | No | Yes | Yes |
| AWS::Events::EventBus | Yes | Yes | Yes | Yes |
| AWS::Events::Rule | Yes | No | Yes | No |
| AWS::FIS::ExperimentTemplate | Yes | No | Yes | No |
| AWS::Glue::Classifier | Yes | Yes | Yes | Yes |
| AWS::Glue::Database | Yes | No | Yes | Yes |
| AWS::Glue::Job | Yes | Yes | Yes | Yes |
| AWS::Glue::MLTransform | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::Glue::Registry | Yes | No | Yes | No |
| AWS::GroundStation::Config | Yes | No | Yes | No |
| AWS::GroundStation ::DataflowEndpointGroup | Yes | No | Yes | No |
| AWS::GroundStation::MissionProfile | Yes | No | Yes | No |
| AWS::GuardDuty::Detector | Yes | Yes | Yes | Yes |
| AWS::GuardDuty::Filter | Yes | No | Yes | No |
| AWS::GuardDuty::IPSet | Yes | No | Yes | Yes |
| AWS::GuardDuty::MalwareProtectionPlan | Yes | Yes | Yes | Yes |
| AWS::GuardDuty::ThreatIntelSet | Yes | Yes | Yes | Yes |
| AWS::IAM::Group | Yes | No | Yes | No |
| AWS::IAM::Policy | Yes | No | Yes | No |
| AWS::IAM::Role | Yes | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::IAM::User | Yes | No | Yes | No |
| AWS::ImageBuilder::ContainerRecipe | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::DistributionConfiguration | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::ImagePipeline | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::ImageRecipe | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::InfrastructureConfiguration | Yes | Yes | Yes | Yes |
| AWS::ImageBuilder::LifecyclePolicy | Yes | No | Yes | Yes |
| AWS::InspectorV2::Activation | Yes | Yes | Yes | Yes |
| AWS::InspectorV2::Filter | Yes | No | Yes | Yes |
| AWS::IoT::AccountAuditConfiguration | No | No | Yes | Yes |
| AWS::IoT::Authorizer | No | No | Yes | Yes |
| AWS::IoT::CACertificate | No | No | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::IoT::CustomMetric | No | No | Yes | Yes |
| AWS::IoT::Dimension | No | No | Yes | Yes |
| AWS::IoT::DomainConfiguration | No | No | Yes | Yes |
| AWS::IoT::FleetMetric | No | No | Yes | Yes |
| AWS::IoT::JobTemplate | No | No | Yes | Yes |
| AWS::IoT::MitigationAction | No | No | Yes | Yes |
| AWS::IoT::Policy | No | No | Yes | Yes |
| AWS::IoT::ProvisioningTemplate | No | No | Yes | Yes |
| AWS::IoT::RoleAlias | No | No | Yes | Yes |
| AWS::IoT::ScheduledAudit | No | No | Yes | Yes |
| AWS::IoT::SecurityProfile | No | No | Yes | Yes |
| AWS::IoT::ThingGroup | No | No | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::KMS::Alias | Yes | No | Yes | Yes |
| AWS::KMS::Key | Yes | Yes | Yes | Yes |
| AWS::KafkaConnect::CustomPlugin | Yes | No | Yes | Yes |
| AWS::Kinesis::Stream | Yes | No | Yes | Yes |
| AWS::Kinesis::StreamConsumer | Yes | Yes | Yes | Yes |
| AWS::KinesisAnalyticsV2::Application | Yes | Yes | Yes | Yes |
| AWS::KinesisFirehose::DeliveryStream | Yes | Yes | Yes | Yes |
| AWS::KinesisVideo::SignalingChannel | No | No | Yes | No |
| AWS::KinesisVideo::Stream | No | No | Yes | No |
| AWS::Lambda::CodeSigningConfig | Yes | No | Yes | No |
| AWS::Lambda::Function | Yes | Yes | Yes | Yes |
| AWS::Lex::Bot | Yes | No | No | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::Lex::BotAlias | Yes | No | No | No |
| AWS::Logs::Destination | Yes | Yes | Yes | Yes |
| AWS::MSK::BatchScramSecret | Yes | No | Yes | Yes |
| AWS::MSK::Cluster | Yes | No | Yes | Yes |
| AWS::MSK::ClusterPolicy | Yes | Yes | Yes | Yes |
| AWS::MSK::Configuration | Yes | Yes | Yes | Yes |
| AWS::MSK::VpcConnection | Yes | Yes | Yes | Yes |
| AWS::Macie::Session | Yes | Yes | Yes | No |
| AWS::MediaConnect::FlowEntitlement | Yes | No | No | Yes |
| AWS::MediaConnect::FlowSource | Yes | No | No | Yes |
| AWS::MediaConnect::FlowVpcInterface | Yes | No | No | Yes |
| AWS::MediaConnect::Gateway | Yes | No | No | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::MediaLive::Multiplexprogram | No | No | No | Yes |
| AWS::MediaPackage::Asset | No | No | No | Yes |
| AWS::MediaPackage::PackagingConfiguration | No | No | No | Yes |
| AWS::MediaPackage::PackagingGroup | No | No | No | Yes |
| AWS::MediaPackageV2::Channel | No | No | No | Yes |
| AWS::MediaPackageV2::ChannelGroup | No | No | No | Yes |
| AWS::MediaPackageV2::OriginEndpoint | No | No | No | Yes |
| AWS::MediaTailor::LiveSource | Yes | No | No | Yes |
| AWS::MediaTailor::PlaybackConfiguration | Yes | No | No | Yes |
| AWS::NetworkFirewall::Firewall | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::FirewallPolicy | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::RuleGroup | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::NetworkFirewall::TLSInspectionConfiguration | Yes | Yes | Yes | Yes |
| AWS::NetworkFirewall::VpcEndpointAssociation | Yes | Yes | Yes | Yes |
| AWS::Omics::RunGroup | No | Yes | No | No |
| AWS::Omics::Workflow | No | Yes | No | No |
| AWS::OpenSearch::Domain | Yes | No | Yes | No |
| AWS::PCAConnectorAD::Connector | Yes | Yes | Yes | Yes |
| AWS::PCAConnectorAD::DirectoryRegistration | Yes | Yes | Yes | Yes |
| AWS::QuickSight::Dashboard | Yes | No | No | No |
| AWS::RDS::DBCluster | Yes | Yes | Yes | Yes |
| AWS::RDS::DBClusterSnapshot | Yes | No | Yes | Yes |
| AWS::RDS::DBInstance | Yes | Yes | Yes | Yes |
| AWS::RDS::DBProxyEndpoint | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::RDS::DBSecurityGroup | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSnapshot | Yes | Yes | Yes | Yes |
| AWS::RDS::DBSubnetGroup | Yes | Yes | Yes | Yes |
| AWS::RDS::EventSubscription | Yes | Yes | Yes | Yes |
| AWS::RDS::GlobalCluster | Yes | Yes | Yes | Yes |
| AWS::RDS::Integration | Yes | Yes | Yes | Yes |
| AWS::RDS::OptionGroup | Yes | Yes | Yes | Yes |
| AWS::RUM::AppMonitor | Yes | No | Yes | Yes |
| AWS::Redshift::Cluster | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterParameterGroup | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSecurityGroup | Yes | Yes | Yes | Yes |
| AWS::Redshift::ClusterSnapshot | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::Redshift::ClusterSubnetGroup | Yes | Yes | Yes | Yes |
| AWS::Redshift::EndpointAccess | Yes | No | Yes | No |
| AWS::Redshift::EndpointAuthorization | Yes | No | Yes | No |
| AWS::Redshift::EventSubscription | Yes | Yes | Yes | Yes |
| AWS::Redshift::Integration | Yes | Yes | Yes | Yes |
| AWS::Redshift::ScheduledAction | No | No | Yes | No |
| AWS::ResilienceHub::App | Yes | No | Yes | No |
| AWS::ResilienceHub::ResiliencyPolicy | Yes | No | Yes | No |
| AWS::ResourceExplorer2::Index | Yes | No | Yes | Yes |
| AWS::RolesAnywhere::CRL | Yes | Yes | Yes | Yes |
| AWS::RolesAnywhere::Profile | Yes | Yes | Yes | Yes |
| AWS::RolesAnywhere::TrustAnchor | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::Route53Profiles::Profile | Yes | Yes | Yes | Yes |
| AWS::Route53Profiles::ProfileAssociation | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::FirewallDomainList | Yes | No | Yes | No |
| AWS::Route53Resolver::FirewallRuleGroup | Yes | No | Yes | No |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverEndpoint | Yes | No | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | Yes | Yes | Yes | Yes |
| AWS::Route53Resolver::ResolverRule | Yes | No | Yes | Yes |
| AWS::Route53Resolver::ResolverRuleAssociation | Yes | No | Yes | Yes |
| AWS::S3::AccessGrant | Yes | Yes | Yes | Yes |
| AWS::S3::AccessGrantsInstance | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::S3::AccessGrantsLocation | Yes | Yes | Yes | Yes |
| AWS::S3::AccessPoint | Yes | Yes | Yes | Yes |
| AWS::S3::AccountPublicAccessBlock | Yes | No | Yes | Yes |
| AWS::S3::Bucket | Yes | Yes | Yes | Yes |
| AWS::S3Tables::TableBucket | Yes | Yes | Yes | Yes |
| AWS::S3Tables::TableBucketPolicy | Yes | Yes | Yes | Yes |
| AWS::SES::ConfigurationSet | Yes | Yes | Yes | Yes |
| AWS::SES::ContactList | Yes | Yes | Yes | Yes |
| AWS::SES::DedicatedIpPool | Yes | Yes | Yes | Yes |
| AWS::SES::MailManagerTrafficPolicy | Yes | No | Yes | Yes |
| AWS::SES::ReceiptFilter | Yes | No | Yes | No |
| AWS::SES::ReceiptRuleSet | Yes | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::SES::Template | Yes | Yes | Yes | Yes |
| AWS::SNS::Topic | Yes | Yes | Yes | Yes |
| AWS::SQS::Queue | Yes | No | Yes | No |
| AWS::SSM::AssociationCompliance | Yes | Yes | Yes | Yes |
| AWS::SSM::Document | Yes | Yes | Yes | Yes |
| AWS::SSM::FileData | Yes | Yes | Yes | Yes |
| AWS::SSM::ManagedInstanceInventory | Yes | Yes | Yes | Yes |
| AWS::SSM::PatchCompliance | Yes | Yes | Yes | Yes |
| AWS::SSM::ResourceDataSync | Yes | Yes | Yes | Yes |
| AWS::SageMaker::AppImageConfig | Yes | Yes | Yes | Yes |
| AWS::SageMaker::CodeRepository | Yes | No | Yes | No |
| AWS::SageMaker::DataQualityJobDefinition | No | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::SageMaker::Domain | Yes | No | Yes | No |
| AWS::SageMaker::EndpointConfig | Yes | No | Yes | No |
| AWS::SageMaker::FeatureGroup | Yes | Yes | Yes | No |
| AWS::SageMaker::Image | Yes | Yes | Yes | Yes |
| AWS::SageMaker::InferenceExperiment | Yes | No | Yes | No |
| AWS::SageMaker::MlflowTrackingServer | Yes | Yes | Yes | Yes |
| AWS::SageMaker::Model | Yes | No | Yes | No |
| AWS::SageMaker::ModelBiasJobDefinition | No | No | Yes | No |
| AWS::SageMaker::ModelExplainabilityJobDefinition | No | No | Yes | No |
| AWS::SageMaker::ModelQualityJobDefinition | No | No | Yes | No |
| AWS::SageMaker::MonitoringSchedule | No | No | Yes | No |
| AWS::SageMaker::NotebookInstance | Yes | No | Yes | No |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::SageMaker::NotebookInstanceLifecycleConfig | Yes | No | Yes | No |
| AWS::SageMaker::StudioLifecycleConfig | Yes | Yes | Yes | Yes |
| AWS::SageMaker::UserProfile | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::ResourcePolicy | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::RotationSchedule | Yes | Yes | Yes | Yes |
| AWS::SecretsManager::Secret | Yes | Yes | Yes | Yes |
| AWS::SecurityHub::Standard | Yes | Yes | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProduct | Yes | No | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | Yes | No | Yes | Yes |
| AWS::ServiceCatalog::Portfolio | Yes | No | Yes | Yes |
| AWS::ServiceDiscovery::HttpNamespace | Yes | Yes | Yes | Yes |
| AWS::ServiceDiscovery::Instance | Yes | No | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::ServiceDiscovery::PublicDnsNamespace | Yes | Yes | Yes | Yes |
| AWS::ServiceDiscovery::Service | Yes | No | Yes | Yes |
| AWS::ShieldRegional::Protection | Yes | Yes | Yes | Yes |
| AWS::Signer::SigningProfile | Yes | No | Yes | No |
| AWS::StepFunctions::Activity | Yes | Yes | Yes | Yes |
| AWS::StepFunctions::StateMachine | Yes | Yes | Yes | Yes |
| AWS::Transfer::Agreement | Yes | No | Yes | Yes |
| AWS::Transfer::Certificate | Yes | Yes | Yes | Yes |
| AWS::Transfer::Connector | Yes | Yes | Yes | Yes |
| AWS::Transfer::Profile | Yes | Yes | Yes | Yes |
| AWS::Transfer::Server | Yes | Yes | Yes | Yes |
| AWS::Transfer::Workflow | Yes | Yes | Yes | Yes |

| Resource type | Africa (Cape Town) | Israel (Tel Aviv) | Middle East (Bahrain) | Middle East (UAE) |
|---|---|---|---|---|
| AWS::WAFRegional::RateBasedRule | Yes | Yes | Yes | Yes |
| AWS::WAFRegional::Rule | Yes | Yes | Yes | Yes |
| AWS::WAFRegional::RuleGroup | Yes | Yes | Yes | Yes |
| AWS::WAFRegional::WebACL | Yes | Yes | Yes | Yes |
| AWS::WAFv2::IPSet | Yes | Yes | Yes | Yes |
| AWS::WAFv2::ManagedRuleSet | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RegexPatternSet | Yes | Yes | Yes | Yes |
| AWS::WAFv2::RuleGroup | Yes | Yes | Yes | Yes |
| AWS::WAFv2::WebACL | Yes | Yes | Yes | Yes |
| AWS::WorkSpaces::Workspace | Yes | No | No | No |
| AWS::XRay::EncryptionConfig | Yes | Yes | No | Yes |

# GovCloud Regions

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::ACM::Certificate | Yes | Yes |
| AWS::ACMPCA::CertificateAuthority | Yes | Yes |
| AWS::ACMPCA::CertificateAuthorityActivation | Yes | Yes |
| AWS::AccessAnalyzer::Analyzer | Yes | Yes |
| AWS::AmazonMQ::Broker | Yes | Yes |
| AWS::ApiGateway::DomainName | Yes | Yes |
| AWS::ApiGateway::Method | Yes | Yes |
| AWS::ApiGateway::RestApi | Yes | Yes |
| AWS::ApiGateway::Stage | Yes | Yes |
| AWS::ApiGateway::UsagePlan | Yes | Yes |
| AWS::ApiGatewayV2::Api | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::ApiGatewayV2::Integration | Yes | Yes |
| AWS::ApiGatewayV2::Stage | Yes | Yes |
| AWS::AppConfig::Application | Yes | Yes |
| AWS::AppConfig::ConfigurationProfile | Yes | Yes |
| AWS::AppConfig::DeploymentStrategy | Yes | Yes |
| AWS::AppConfig::Environment | Yes | Yes |
| AWS::AppConfig::Extension | Yes | Yes |
| AWS::AppConfig::ExtensionAssociation | Yes | Yes |
| AWS::AppConfig::HostedConfigurationVersion | Yes | Yes |
| AWS::AppStream::AppBlockBuilder | Yes | Yes |
| AWS::AppStream::Application | Yes | Yes |
| AWS::AppStream::DirectoryConfig | Yes | No |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::AppStream::Fleet | Yes | No |
| AWS::AppStream::Stack | Yes | No |
| AWS::Athena::DataCatalog | Yes | Yes |
| AWS::Athena::WorkGroup | Yes | Yes |
| AWS::AutoScaling::AutoScalingGroup | Yes | Yes |
| AWS::AutoScaling::LaunchConfiguration | Yes | Yes |
| AWS::AutoScaling::ScalingPolicy | Yes | Yes |
| AWS::AutoScaling::ScheduledAction | Yes | Yes |
| AWS::AutoScaling::WarmPool | Yes | Yes |
| AWS::Backup::BackupPlan | Yes | Yes |
| AWS::Backup::BackupSelection | Yes | Yes |
| AWS::Backup::BackupVault | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::Backup::RecoveryPoint | Yes | Yes |
| AWS::BackupGateway::Hypervisor | Yes | Yes |
| AWS::Batch::ComputeEnvironment | Yes | Yes |
| AWS::Batch::JobQueue | Yes | Yes |
| AWS::Batch::SchedulingPolicy | Yes | Yes |
| AWS::Bedrock::Guardrail | Yes | Yes |
| AWS::Bedrock::KnowledgeBase | Yes | Yes |
| AWS::Bedrock::Prompt | Yes | Yes |
| AWS::Cassandra::Keyspace | Yes | Yes |
| AWS::CloudFormation::Stack | Yes | Yes |
| AWS::CloudFormation::StackSet | Yes | Yes |
| AWS::CloudTrail::EventDataStore | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::CloudTrail::Trail | Yes | Yes |
| AWS::CloudWatch::Alarm | Yes | Yes |
| AWS::CodeBuild::Project | Yes | Yes |
| AWS::CodeBuild::ReportGroup | Yes | Yes |
| AWS::Cognito::IdentityPool | Yes | No |
| AWS::Cognito::UserPoolGroup | Yes | No |
| AWS::Config::ConfigurationRecorder | Yes | Yes |
| AWS::Config::ConformancePack | Yes | Yes |
| AWS::Config::ConformancePackCompliance | Yes | Yes |
| AWS::Config::ResourceCompliance | Yes | Yes |
| AWS::Config::StoredQuery | Yes | Yes |
| AWS::Connect::Instance | Yes | No |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::Connect::QuickConnect | Yes | No |
| AWS::Connect::SecurityProfile | Yes | No |
| AWS::Connect::User | Yes | No |
| AWS::DMS::Certificate | Yes | Yes |
| AWS::DMS::Endpoint | Yes | Yes |
| AWS::DMS::EventSubscription | Yes | Yes |
| AWS::DMS::ReplicationInstance | Yes | Yes |
| AWS::DMS::ReplicationSubnetGroup | Yes | Yes |
| AWS::DMS::ReplicationTask | Yes | Yes |
| AWS::DataSync::Agent | Yes | Yes |
| AWS::DataSync::LocationEFS | Yes | Yes |
| AWS::DataSync::LocationFSxLustre | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::DataSync::LocationFSxWindows | Yes | Yes |
| AWS::DataSync::LocationHDFS | Yes | Yes |
| AWS::DataSync::LocationNFS | Yes | Yes |
| AWS::DataSync::LocationObjectStorage | Yes | Yes |
| AWS::DataSync::LocationS3 | Yes | Yes |
| AWS::DataSync::LocationSMB | Yes | Yes |
| AWS::DataSync::Task | Yes | Yes |
| AWS::Detective::Graph | Yes | Yes |
| AWS::DynamoDB::Table | Yes | Yes |
| AWS::EC2::CapacityReservation | Yes | Yes |
| AWS::EC2::ClientVpnEndpoint | Yes | Yes |
| AWS::EC2::ClientVpnTargetNetworkAssociation | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::EC2::CustomerGateway | Yes | Yes |
| AWS::EC2::DHCPOptions | Yes | Yes |
| AWS::EC2::EC2Fleet | Yes | Yes |
| AWS::EC2::EIP | Yes | Yes |
| AWS::EC2::EgressOnlyInternetGateway | Yes | Yes |
| AWS::EC2::FlowLog | Yes | Yes |
| AWS::EC2::Host | Yes | Yes |
| AWS::EC2::IPAM | Yes | Yes |
| AWS::EC2::IPAMPool | Yes | Yes |
| AWS::EC2::IPAMPoolCidr | Yes | Yes |
| AWS::EC2::IPAMResourceDiscovery | Yes | Yes |
| AWS::EC2::IPAMResourceDiscoveryAssociation | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::EC2::IPAMScope | Yes | Yes |
| AWS::EC2::Instance | Yes | Yes |
| AWS::EC2::InstanceConnectEndpoint | Yes | Yes |
| AWS::EC2::InternetGateway | Yes | Yes |
| AWS::EC2::LaunchTemplate | Yes | Yes |
| AWS::EC2::NatGateway | Yes | Yes |
| AWS::EC2::NetworkAcl | Yes | Yes |
| AWS::EC2::NetworkInterface | Yes | Yes |
| AWS::EC2::PrefixList | Yes | Yes |
| AWS::EC2::RouteTable | Yes | Yes |
| AWS::EC2::SecurityGroup | Yes | Yes |
| AWS::EC2::SecurityGroupVpcAssociation | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::EC2::SnapshotBlockPublicAccess | Yes | Yes |
| AWS::EC2::SpotFleet | Yes | Yes |
| AWS::EC2::Subnet | Yes | Yes |
| AWS::EC2::SubnetCidrBlock | Yes | Yes |
| AWS::EC2::SubnetNetworkAclAssociation | Yes | Yes |
| AWS::EC2::SubnetRouteTableAssociation | Yes | Yes |
| AWS::EC2::TrafficMirrorFilter | Yes | Yes |
| AWS::EC2::TrafficMirrorSession | Yes | Yes |
| AWS::EC2::TrafficMirrorTarget | Yes | Yes |
| AWS::EC2::TransitGateway | Yes | No |
| AWS::EC2::TransitGatewayAttachment | Yes | Yes |
| AWS::EC2::TransitGatewayConnect | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::EC2::TransitGatewayMulticastDomain | Yes | Yes |
| AWS::EC2::TransitGatewayRouteTable | Yes | Yes |
| AWS::EC2::VPC | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessExclusion | Yes | Yes |
| AWS::EC2::VPCBlockPublicAccessOptions | Yes | Yes |
| AWS::EC2::VPCEndpoint | Yes | Yes |
| AWS::EC2::VPCEndpointConnectionNotification | Yes | Yes |
| AWS::EC2::VPCEndpointService | Yes | No |
| AWS::EC2::VPCGatewayAttachment | Yes | Yes |
| AWS::EC2::VPCPeeringConnection | Yes | Yes |
| AWS::EC2::VPNConnection | Yes | Yes |
| AWS::EC2::VPNConnectionRoute | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::EC2::VPNGateway | Yes | Yes |
| AWS::EC2::VerifiedAccessInstance | Yes | Yes |
| AWS::EC2::Volume | Yes | Yes |
| AWS::ECR::ReplicationConfiguration | Yes | Yes |
| AWS::ECR::Repository | Yes | Yes |
| AWS::ECS::CapacityProvider | Yes | Yes |
| AWS::ECS::Cluster | Yes | Yes |
| AWS::ECS::Service | Yes | Yes |
| AWS::ECS::TaskDefinition | Yes | Yes |
| AWS::ECS::TaskSet | Yes | Yes |
| AWS::EFS::AccessPoint | Yes | Yes |
| AWS::EFS::FileSystem | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::EKS::Addon | Yes | Yes |
| AWS::EKS::Cluster | Yes | Yes |
| AWS::EKS::IdentityProviderConfig | Yes | Yes |
| AWS::EMR::SecurityConfiguration | Yes | Yes |
| AWS::EMR::Studio | Yes | Yes |
| AWS::EMRContainers::VirtualCluster | Yes | Yes |
| AWS::ElasticBeanstalk::Application | Yes | Yes |
| AWS::ElasticBeanstalk::ApplicationVersion | Yes | Yes |
| AWS::ElasticBeanstalk::Environment | Yes | Yes |
| AWS::ElasticLoadBalancing::LoadBalancer | Yes | Yes |
| AWS::ElasticLoadBalancingV2::Listener | Yes | Yes |
| AWS::ElasticLoadBalancingV2::LoadBalancer | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::ElasticLoadBalancingV2::TargetGroup | Yes | Yes |
| AWS::Elasticsearch::Domain | Yes | Yes |
| AWS::Events::EventBus | Yes | Yes |
| AWS::Events::Rule | Yes | Yes |
| AWS::FIS::ExperimentTemplate | Yes | Yes |
| AWS::Glue::Classifier | Yes | Yes |
| AWS::Glue::Job | Yes | Yes |
| AWS::Glue::MLTransform | Yes | No |
| AWS::Glue::Registry | Yes | Yes |
| AWS::GreengrassV2::ComponentVersion | Yes | Yes |
| AWS::GuardDuty::Detector | Yes | Yes |
| AWS::GuardDuty::Filter | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::GuardDuty::IPSet | Yes | Yes |
| AWS::GuardDuty::ThreatIntelSet | Yes | Yes |
| AWS::IAM::Group | Yes | Yes |
| AWS::IAM::InstanceProfile | No | Yes |
| AWS::IAM::OIDCProvider | No | Yes |
| AWS::IAM::Policy | Yes | Yes |
| AWS::IAM::Role | Yes | Yes |
| AWS::IAM::SAMLProvider | No | Yes |
| AWS::IAM::ServerCertificate | No | Yes |
| AWS::IAM::User | Yes | Yes |
| AWS::ImageBuilder::ContainerRecipe | Yes | Yes |
| AWS::ImageBuilder::DistributionConfiguration | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::ImageBuilder::ImagePipeline | Yes | Yes |
| AWS::ImageBuilder::ImageRecipe | Yes | Yes |
| AWS::ImageBuilder::InfrastructureConfiguration | Yes | Yes |
| AWS::InspectorV2::Activation | Yes | Yes |
| AWS::IoT::AccountAuditConfiguration | Yes | Yes |
| AWS::IoT::Authorizer | Yes | Yes |
| AWS::IoT::CACertificate | Yes | Yes |
| AWS::IoT::CustomMetric | Yes | Yes |
| AWS::IoT::Dimension | Yes | Yes |
| AWS::IoT::FleetMetric | Yes | Yes |
| AWS::IoT::JobTemplate | Yes | Yes |
| AWS::IoT::MitigationAction | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::IoT::Policy | Yes | Yes |
| AWS::IoT::ProvisioningTemplate | Yes | Yes |
| AWS::IoT::RoleAlias | Yes | Yes |
| AWS::IoT::ScheduledAudit | Yes | Yes |
| AWS::IoT::SecurityProfile | Yes | Yes |
| AWS::IoT::ThingGroup | Yes | Yes |
| AWS::IoTEvents::AlarmModel | Yes | No |
| AWS::IoTEvents::DetectorModel | Yes | No |
| AWS::IoTEvents::Input | Yes | No |
| AWS::IoTSiteWise::Asset | Yes | No |
| AWS::IoTSiteWise::AssetModel | Yes | No |
| AWS::IoTSiteWise::Gateway | Yes | No |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::IoTSiteWise::Portal | Yes | No |
| AWS::IoTTwinMaker::ComponentType | Yes | No |
| AWS::IoTTwinMaker::Entity | Yes | No |
| AWS::IoTTwinMaker::Workspace | Yes | No |
| AWS::KMS::Alias | Yes | Yes |
| AWS::KMS::Key | Yes | Yes |
| AWS::Kinesis::Stream | Yes | Yes |
| AWS::Kinesis::StreamConsumer | Yes | Yes |
| AWS::KinesisAnalyticsV2::Application | Yes | Yes |
| AWS::KinesisFirehose::DeliveryStream | Yes | Yes |
| AWS::Lambda::Function | Yes | Yes |
| AWS::Location::GeofenceCollection | Yes | No |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::Location::Map | Yes | No |
| AWS::Location::PlaceIndex | Yes | No |
| AWS::Location::RouteCalculator | Yes | No |
| AWS::Logs::Destination | Yes | Yes |
| AWS::MSK::BatchScramSecret | Yes | Yes |
| AWS::MSK::Cluster | Yes | Yes |
| AWS::MSK::ClusterPolicy | Yes | Yes |
| AWS::MSK::Configuration | Yes | Yes |
| AWS::MSK::VpcConnection | Yes | Yes |
| AWS::NetworkFirewall::Firewall | Yes | Yes |
| AWS::NetworkFirewall::FirewallPolicy | Yes | Yes |
| AWS::NetworkFirewall::RuleGroup | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::NetworkFirewall::VpcEndpointAssociation | Yes | Yes |
| AWS::NetworkManager::CustomerGatewayAssociation | Yes | No |
| AWS::NetworkManager::Device | Yes | No |
| AWS::NetworkManager::GlobalNetwork | Yes | No |
| AWS::NetworkManager::Link | Yes | No |
| AWS::NetworkManager::LinkAssociation | Yes | No |
| AWS::NetworkManager::Site | Yes | No |
| AWS::NetworkManager::TransitGatewayRegistration | Yes | No |
| AWS::OpenSearch::Domain | Yes | Yes |
| AWS::OpenSearchServerless::SecurityConfig | Yes | Yes |
| AWS::Pinpoint::App | Yes | No |
| AWS::Pinpoint::ApplicationSettings | Yes | No |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::Pinpoint::Campaign | Yes | No |
| AWS::Pinpoint::EmailChannel | Yes | No |
| AWS::Pinpoint::EmailTemplate | Yes | No |
| AWS::Pinpoint::EventStream | Yes | No |
| AWS::Pinpoint::InAppTemplate | Yes | No |
| AWS::Pinpoint::Segment | Yes | No |
| AWS::QuickSight::Dashboard | Yes | Yes |
| AWS::QuickSight::Template | Yes | No |
| AWS::RDS::DBCluster | Yes | Yes |
| AWS::RDS::DBClusterSnapshot | Yes | Yes |
| AWS::RDS::DBInstance | Yes | Yes |
| AWS::RDS::DBProxyEndpoint | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::RDS::DBSecurityGroup | Yes | Yes |
| AWS::RDS::DBSnapshot | Yes | Yes |
| AWS::RDS::DBSubnetGroup | Yes | Yes |
| AWS::RDS::EventSubscription | Yes | Yes |
| AWS::RDS::OptionGroup | Yes | Yes |
| AWS::Redshift::Cluster | Yes | Yes |
| AWS::Redshift::ClusterParameterGroup | Yes | Yes |
| AWS::Redshift::ClusterSecurityGroup | Yes | Yes |
| AWS::Redshift::ClusterSnapshot | Yes | Yes |
| AWS::Redshift::ClusterSubnetGroup | Yes | Yes |
| AWS::Redshift::EventSubscription | Yes | Yes |
| AWS::Redshift::Integration | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::Redshift::ScheduledAction | Yes | Yes |
| AWS::RoboMaker::RobotApplication | Yes | No |
| AWS::RoboMaker::RobotApplicationVersion | Yes | No |
| AWS::RoboMaker::SimulationApplication | Yes | No |
| AWS::RolesAnywhere::CRL | Yes | Yes |
| AWS::RolesAnywhere::Profile | Yes | Yes |
| AWS::RolesAnywhere::TrustAnchor | Yes | Yes |
| AWS::Route53Profiles::Profile | Yes | Yes |
| AWS::Route53Profiles::ProfileAssociation | Yes | Yes |
| AWS::Route53Resolver::FirewallDomainList | Yes | Yes |
| AWS::Route53Resolver::FirewallRuleGroup | Yes | Yes |
| AWS::Route53Resolver::FirewallRuleGroupAssociation | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::Route53Resolver::ResolverEndpoint | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfig | Yes | Yes |
| AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation | Yes | Yes |
| AWS::Route53Resolver::ResolverRule | Yes | Yes |
| AWS::Route53Resolver::ResolverRuleAssociation | Yes | Yes |
| AWS::S3::AccessGrant | Yes | Yes |
| AWS::S3::AccessGrantsInstance | Yes | Yes |
| AWS::S3::AccessGrantsLocation | Yes | Yes |
| AWS::S3::AccessPoint | Yes | Yes |
| AWS::S3::AccountPublicAccessBlock | Yes | Yes |
| AWS::S3::Bucket | Yes | Yes |
| AWS::SES::ConfigurationSet | Yes | No |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::SES::ContactList | Yes | No |
| AWS::SES::DedicatedIpPool | Yes | Yes |
| AWS::SES::Template | Yes | No |
| AWS::SNS::Topic | Yes | Yes |
| AWS::SQS::Queue | Yes | Yes |
| AWS::SSM::AssociationCompliance | Yes | Yes |
| AWS::SSM::Document | Yes | Yes |
| AWS::SSM::FileData | Yes | Yes |
| AWS::SSM::ManagedInstanceInventory | Yes | Yes |
| AWS::SSM::PatchCompliance | Yes | Yes |
| AWS::SSM::ResourceDataSync | Yes | Yes |
| AWS::SageMaker::Model | Yes | No |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::SageMaker::NotebookInstance | Yes | No |
| AWS::SageMaker::NotebookInstanceLifecycleConfig | Yes | No |
| AWS::SageMaker::StudioLifecycleConfig | Yes | Yes |
| AWS::SageMaker::UserProfile | Yes | Yes |
| AWS::SecretsManager::ResourcePolicy | Yes | Yes |
| AWS::SecretsManager::RotationSchedule | Yes | Yes |
| AWS::SecretsManager::Secret | Yes | Yes |
| AWS::SecurityHub::Standard | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProduct | Yes | Yes |
| AWS::ServiceCatalog::CloudFormationProvisionedProduct | Yes | Yes |
| AWS::ServiceCatalog::Portfolio | Yes | Yes |
| AWS::ServiceDiscovery::HttpNamespace | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::ServiceDiscovery::Instance | Yes | Yes |
| AWS::ServiceDiscovery::Service | Yes | Yes |
| AWS::StepFunctions::StateMachine | Yes | Yes |
| AWS::Transfer::Agreement | Yes | Yes |
| AWS::Transfer::Certificate | Yes | Yes |
| AWS::Transfer::Connector | Yes | Yes |
| AWS::Transfer::Profile | Yes | Yes |
| AWS::Transfer::Server | Yes | Yes |
| AWS::Transfer::Workflow | Yes | Yes |
| AWS::WAFRegional::RateBasedRule | Yes | Yes |
| AWS::WAFRegional::Rule | Yes | Yes |
| AWS::WAFRegional::RuleGroup | Yes | Yes |

| Resource type | AWS GovCloud (US-West) | AWS GovCloud (US-East) |
|---|---|---|
| AWS::WAFRegional::WebACL | Yes | Yes |
| AWS::WAFv2::IPSet | Yes | Yes |
| AWS::WAFv2::ManagedRuleSet | Yes | Yes |
| AWS::WAFv2::RegexPatternSet | Yes | Yes |
| AWS::WAFv2::RuleGroup | Yes | Yes |
| AWS::WAFv2::WebACL | Yes | Yes |
| AWS::WorkSpaces::Workspace | Yes | No |

# Recording AWS Resources with AWS Config

AWS Config continuously detects when supported resource types are created, changed, or deleted. AWS Config records these events as configuration items (CIs).

You can customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. For a list of supported resource types that AWS Config can record, see Supported Resource Types for AWS Config.

**Topics**


- Considerations
- What are the differences between Regional and global resources?
- AWS Config Rules and global resource types

- Recording frequency for AWS Config
- Non-recorded resources
- Recording resources in the AWS Config console
- Recording resources with the AWS CLI
- Excluding resources from recording with AWS Config
- Stopping AWS Config from recording with the customer managed configuration recorder

## Considerations

### High Number of AWS Config Evaluations

You might notice increased activity in your account during your initial month recording with AWS Config when compared to subsequent months. During the initial bootstrapping process, AWS Config runs evaluations on all the resources in your account that you have selected for AWS Config to record.

If you are running ephemeral workloads, you may see increased activity from AWS Config as it records configuration changes associated with creating and deleting these temporary resources. An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and AWS Auto Scaling.

If you want to avoid the increased activity from running ephemeral workloads, you can set up the customer managed configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with AWS Config turned off to avoid increased configuration recording and rule evaluations.

### Region availability

Before specifying a resource type for AWS Config to track, check Resource Coverage by Region availability to see if the resource type is supported in the AWS Region where you set up AWS Config.

If a resource type is supported by AWS Config in at least one Region, you can enable the recording of that resource type in all Regions supported by AWS Config, even if the specified resource type is not supported in the AWS Region where you set up AWS Config.

## What are the differences between Regional and global resources?

### Regional resources

*Regional resources* are tied to a Region and can be used only in that Region. You create them in a specified AWS Region, and then they exist in that Region. To see or interact with those resources, you must direct your operations to that Region. For example, to create an Amazon EC2 instance with the AWS Management Console, you choose the AWS Region that you want to create the instance in. If you use the AWS Command Line Interface (AWS CLI) to create the instance, then you include the `--region` parameter. The AWS SDKs each have their own equivalent mechanism to specify the Region that the operation uses.

There are several reasons for using Regional resources. One reason is to ensure that the resources, and the service endpoints that you use to access them, are as close to the customer as possible. This improves performance by minimizing latency. Another reason is to provide an isolation boundary. This lets you create independent copies of resources in multiple Regions to distribute the load and improve scalability. At the same time, it isolates the resources from each other to improve availability.

If you specify a different AWS Region in the console or in an AWS CLI command, then you can no longer see or interact with the resources you could see in the previous Region.

When you look at the Amazon Resource Name (ARN) for a Regional resource, the Region that contains the resource is specified as the fourth field in the ARN. For example, an Amazon EC2 instance is a Regional resource. The following is an example of an ARN for a Amazon EC2 instance that exists in the `us-east-1` Region.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

### Global resources

Some AWS services resources are *global resources*, meaning that you can use the resource from ***anywhere***. You don't specify an AWS Region in a global service's console. To access a global resource, you don't specify a `--region` parameter when using the service's AWS CLI and AWS SDK operations.

Global resources support cases where it is critical that only one instance of a particular resource can exist at a time. In these scenarios, replication or synchronization between copies in different Regions is not adequate. Having to access a single global endpoint, with the possible increase

in latency, is considered acceptable to ensure that any changes are instantaneously visible to consumers of the resource.

For example, Amazon Aurora global clusters (`AWS::RDS::GlobalCluster`) are global resources, and therefore not tied to a Region. This means that you can create a global cluster without relying on a regional endpoint. The benefit is that, while the Amazon Relational Database Service (Amazon RDS) itself is organized by Regions, the specific Region where a global cluster originates doesn't impact the global cluster. It appears as a single, continuous global cluster across all Regions.

The Amazon Resource Name (ARN) for a global resource doesn't include a Region. The fourth field is empty, such as in the following example of an ARN for a global cluster.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> Global resource types onboarded to AWS Config after February 2022 will only be recorded in the service's home Region for the commercial partition and AWS GovCloud (US-West) for the GovCloud partition. You can view the configuration items (CIs) for these new global resource types only in their home Region and AWS GovCloud (US-West).
>
> Global resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) remain unchanged. You can enable the recording of these global IAM resources in all Regions where AWS Config was supported before February 2022. These global IAM resources cannot be recorded in Regions supported by AWS Config after February 2022.

### Global resource types | IAM resources

The following IAM resource types are global resources: IAM users, groups, roles, and customer managed policies. These resource types can be recorded by AWS Config in Regions where AWS Config was available before February 2022. This list where you cannot record the global IAM resource types includes the following Regions: Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Asia Pacific (Thailand), Canada West (Calgary), Europe (Spain), Europe (Zurich), Israel (Tel Aviv), Mexico (Central), and Middle East (UAE).

To prevent duplicate configuration items (CIs), you should consider only recording the global IAM resource types one time in one of the supported Regions. This can also help you avoid unneccessary evaluations and API throttling.

**Global resource types | Home Region Only**

Global resources for the following services are only recorded by AWS Config in the home Region of the global resource type: Amazon Elastic Container Registry Public, AWS Global Accelerator, Amazon Route 53, Amazon CloudFront, and AWS WAF. For these global resources, the same instance of the resource type can be used in multiple AWS Regions, but the configuration items (CIs) are only recorded in the home Region for the commercial partition or AWS GovCloud (US-West) for the AWS GovCloud (US) partition.

**Home Regions for Global Resource Types**

| AWS Service | Resource Type Value | Home Region |
| --- | --- | --- |
| Amazon Elastic Container Registry Public | `AWS::ECR::PublicRepository` | US East (N. Virginia) Region |
| AWS Global Accelerator | `AWS::GlobalAccelerator::Listener` | US West (Oregon) Region |
| | `AWS::GlobalAccelerator::EndpointGroup` | US West (Oregon) Region |
| | `AWS::GlobalAccelerator::Accelerator` | US West (Oregon) Region |
| Amazon Route 53 | `AWS::Route53::HostedZone` | US East (N. Virginia) Region |
| | `AWS::Route53::HealthCheck` | US East (N. Virginia) Region |
| Amazon CloudFront | `AWS::CloudFront::Distribution` | US East (N. Virginia) Region |
| AWS WAF | `AWS::WAFv2::WebACL` | US East (N. Virginia) Region |

**Global resource types | Aurora global clusters**

`AWS::RDS::GlobalCluster` is a global resource that is recorded in all supported AWS Config Regions where the customer managed configuration recorder is enabled. This global resource type is unique in that if you enable the recording of this resource in one Region, AWS Config will record configuration items (CIs) for this resource type in all your enabled Regions.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, use one of the following recording strategies for the AWS Config console:

- **Record all resource types with customizable overrides**, choose "AWS RDS GlobalCluster", and choose the override "Exclude from recording"
- **Record specific resource types**.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, use one of the following recording strategies for the API/CLI:

- **Record all current and future resource types with exclusions** (`EXCLUSION_BY_RESOURCE_TYPES`)
- **Record specific resource types** (`INCLUSION_BY_RESOURCE_TYPES`).

## AWS Config Rules and global resource types

The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in Regions where AWS Config was available before February 2022. These global IAM resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.

If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.

**Best Practices for reporting compliance on global resources onboarded before February 2022**

To avoid unnecessary evaluations, you should only deploy AWS Config rules and conformance packs that have these global resources in scope to one of the supported Regions. For a list of which

managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability. This applies to AWS Config rules, organizational AWS Config rules, and also rules created by other AWS services, such as AWS Security Hub CSPM and AWS Control Tower.

If you are not recording global resource types onboarded before February 2022, it is recommended that you do not enable the following periodic rules to avoid unnecessary evaluations:

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

**Best Practices for reporting compliance on global resources onboarded after February 2022**

Global resource types onboarded to AWS Config recording after February 2022 will be recorded only in the service's home Region for the commercial partition and AWS GovCloud (US-West) for the AWS GovCloud (US) partition. You should deploy AWS Config rules and conformance packs that have these global resources in scope only to the resource type's home Region. For more information, see Home Regions for Global Resource Types.

## Recording frequency for AWS Config

AWS Config supports *Continuous recording* and *Daily recording*. Continuous recording allows you to record configuration changes continuously whenever a change occurs. Daily recording allows you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it’s different from the previous CI recorded. For steps on how to change the recording frequency, see Changing Recording Frequency.

**Continuous recording**

Some benefits of continuous recording include:

- **Real-time Monitoring**: Continuous recording can provide immediate detection for unauthorized changes or unexpected alterations, which can enhance your security and compliance efforts.
- **Detailed Analysis**: Continuous recording can allow you to perfom in-depth analysis of configuration changes to your resources as they occur, which can allow you to identify patterns and trends in the moment.

### Daily recording

Some benefits of daily recording include:

- **Minimal Disruption**: Daily recording can provide you with a more mangeable flow of information, which can reduce the frequency of notifications and alert fatigue.
- **Cost Efficiency**: Daily recording can provide you with the flexibility to record changes to your resources at at a lower frequency, which can reduce costs related to the number of configuration changes recorded.

> **Note**
>
> AWS Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

## Non-recorded resources

If a resource is not recorded, AWS Config captures only the creation and deletion of that resource, and no other details, at no cost to you. When a non-recorded resource is created or deleted, AWS Config sends a notification, and it displays the event on the resource details page. The details page for a non-recorded resource provides null values for most configuration details, and it does not provide information about relationships and configuration changes.

The relationship information that AWS Config provides for recorded resources is not limited because of missing data for non-recorded resources. If a recorded resource is related to a non-recorded resource, that relationship is provided in the details page of the recorded resource.

### IAM resource type considerations

The `AWS::IAM::User`, `AWS::IAM::Policy`, `AWS::IAM::Group`, `AWS::IAM::Role` resource types will only capture the creation (`ResourceNotRecorded`) and deletion (`ResourceDeletedNotRecorded`) states if the resource is, or previously was, selected as a resource to record in the customer managed configuration recorder .

**CI recording schedule for non-recorded resources**

The configuration items (CIs) for `ResourceNotRecorded` and `ResourceDeletedNotRecorded` do not follow the typical recording time for resource types. These resource types are only recorded during the periodic baselining process for the customer managed configuration recorder, which is at a less frequent cadance than that for the other resource types. This means that create and delete notifications are not sent upon creation or deletion, but during the baselining process.

**CI delivery and service-linked recorder scope**

For service-linked configuration recorders, the recording scope determines if you receive configuration items (CIs) in the delivery channel. The recording scope is set by the service that is linked to the configuration recorder. If the recording scope is internal, you will not receive CIs in the delivery channel.

## Recording resources in the AWS Config console

You can use the AWS Config console to select the types of resources that AWS Config records with the customer managed configuration recorder.

**To select resources**

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the left navigation pane.
3. On the **Customer managed recorder** tab, choose **Edit**.
4. In the **Recording method** section, choose a recording strategy. You can specify the AWS resources that you want AWS Config to record.

   All resource types with customizable overrides

   Set up AWS Config to record configuration changes for all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording. For more information, see Supported Resource Types.

- **Default settings**

  Configure the default recording frequency for all current and future supported resource types. For more information see, Recording Frequency.

  - Continuous recording – AWS Config will record configuration changes continuously whenever a change occurs.
  - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

  > **Note**
  >
  > AWS Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

- **Override settings**

  Override the recording frequency for specific resource types, or exclude specific resource types from recording. If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

Specific resource types

Set up AWS Config to record configuration changes for only the resource types that you specify.

- **Specific resource types**

  Choose a resource type to record and its frequency. For more information see, Recording Frequency.

  - Continuous recording – AWS Config will record configuration changes continuously whenever a change occurs.
  - Daily recording – You will receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded.

> **Note**
>
> AWS Firewall Manager depends on continuous recording to monitor your resources. If you are using Firewall Manager, it is recommended that you set the recording frequency to Continuous.

If you change the recording frequency for a resource type or stop recording a resource type, the configuration items that were already recorded will remain unchanged.

5. Choose **Save** to save your changes.

## Considerations When Recording Resources

### High Number of AWS Config Evaluations

You might notice increased activity in your account during your initial month recording with AWS Config when compared to subsequent months. During the initial bootstrapping process, AWS Config runs evaluations on all the resources in your account that you have selected for AWS Config to record.

If you are running ephemeral workloads, you may see increased activity from AWS Config as it records configuration changes associated with creating and deleting these temporary resources. An *ephemeral workload* is a temporary use of computing resources that are loaded and run when needed. Examples include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances, Amazon EMR jobs, and AWS Auto Scaling. . If you want to avoid the increased activity from running ephemeral workloads, you can set up the customer managed configuration recorder to exclude these resource types from being recorded, or run these types of workloads in a separate account with AWS Config turned off to avoid increased configuration recording and rule evaluations.

Considerations: All resource types with customizable overrides

**Globally recorded resource types | Aurora global clusters are initially included in recording**

The `AWS::RDS::GlobalCluster` resource type will be recorded in all supported AWS Config Regions where the customer managed configuration recorder is enabled.

If you do not want to record `AWS::RDS::GlobalCluster` in all enabled Regions, choose "AWS RDS GlobalCluster", and choose the override "Exclude from recording".

**Global resource types | IAM resource types are initially excluded from recording**

The global IAM resource types are initially excluded from recording to help you reduce costs. This bundle includes IAM users, groups, roles, and customer managed policies. Choose **Remove** to remove the override and include these resources in your recording.

Additionally, the global IAM resource types (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy`) cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.

**Limits**

You can add up to 100 frequency overrides and 600 exclusion overrides.

Daily recording is not supported for the following resource types:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

**Region Availability**

Before specifying a resource type for AWS Config to track, check Resource Coverage by Region Availability to see if the resource type is supported in the AWS Region where you set up AWS Config. If a resource type is supported by AWS Config in at least one Region, you can enable the recording of that resource type in all Regions supported by AWS Config, even if the specified resource type is not supported in the AWS Region where you set up AWS Config.

**Limits**

No limits if all resource types have the same frequency. You can add up to 100 resource types with Daily frequency if at least one resource type is set to Continuous.

The Daily frequency is not supported for the following resource types:

- `AWS::Config::ResourceCompliance`

- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

## Recording resources with the AWS CLI

You can use the AWS CLI to select the types of resources that you want AWS Config to record. You do this by creating a customer managed configuration recorder, which records the types of resources that you specify in a recording group. In the recording group, you specify whether you want to record all supported resource types, or to include or exclude specific types of resources.

Record all current and future supported resource types

Set up AWS Config to record configuration changes for all current and future supported resource types in this Region. For a list of supported resources types, see Supported Resource Types.

1. Use the `put-configuration-recorder` command:

   This command uses the `--configuration-recorder` and `---recording-group` fields.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

   **The `configuration-recorder` field**

   The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`).

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
```

```
        }
    ]
  }
}
```

### The `recording-group` field

The `recordingGroup.json` file specifies which resource types are recorded.

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

For more information about these fields, see `put-configuration-recorder` in the *AWS CLI Command Reference*.

2. (Optional) To verify that your customer managed configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command.

```
$ aws configservice describe-configuration-recorders
```

The following is an example response.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
```

```
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

Set up AWS Config to record configuration changes for all current and future supported resource types, including global resource types, except the resource types that you specify to exclude from recording.

If you choose to stop recording for a resource type, the configuration items that were already recorded will remain unchanged. For a list of supported resources types, see Supported Resource Types.

1. Use the `put-configuration-recorder` command:

   This command uses the `--configuration-recorder` and `---recording-group` fields.

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   **The `configuration-recorder` field**

   The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`).

   ```
   {
     "name": "default",
   ```

```
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

### The `recording-group` field

The `recordingGroup.json` file specifies which types of resources AWS Config will record. Pass one or more resource types to exclude in the `resourceTypes` field of `exclusionByResourceTypes`, as shown in the following example.

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

For more information about these fields, see `put-configuration-recorder` in the *AWS CLI Command Reference*.

2. (Optional) To verify that your customer managed configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command.

```
$ aws configservice describe-configuration-recorders
```

The following is an example response.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Set up AWS Config to record configuration changes for only the resource types that you specify.

If you choose to stop recording for a resource type, the configuration items that were already recorded will remain unchanged. For a list of supported resources types, see Supported Resource Types.

1. Use the `put-configuration-recorder` command:

   This command uses the `--configuration-recorder` and `---recording-group` fields.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

### The `configuration-recorder` field

The `configurationRecorder.json` file specifies `name` and `roleArn` as well as the default recording frequency for the configuration recorder (`recordingMode`).

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

### The `recording-group` field

The `recordingGroup.json` file specifies which types of resources AWS Config will record. Pass one or more resource types to exclude in the `resourceTypes` field as shown in the following example.

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

For more information about these fields, see `put-configuration-recorder` in the *AWS CLI Command Reference*.

2. (Optional) To verify that your customer managed configuration recorder has the settings that you want, use the following `describe-configuration-recorders` command.

```
$ aws configservice describe-configuration-recorders
```

The following is an example response.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
```

```
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

## Excluding resources from recording with AWS Config

AWS Config allows you to exclude specific types of AWS resources from inventory tracking and compliance monitoring while still tracking all other supported resource types currently available in AWS Config, including those that will be added in the future. You can use this feature to concentrate on critical resources that are subject to your compliance and governance standards.

Excluding resources (Console)

If you do not want to record an AWS resource type, use one of the following recording strategies for the AWS Config console:

- **Record all resource types with customizable overrides**, choose the resource type you want to exclude, and choose the override "Exclude from recording"
- **Record specific resource types**.

For more detailed steps, see Recording resources (Console).

Excluding resources (AWS CLI)

If you do not want to record an AWS resource type, use one of the following recording strategies for the API/CLI:

- **Record all current and future resource types with exclusions** (`EXCLUSION_BY_RESOURCE_TYPES`)
- **Record specific resource types** (`INCLUSION_BY_RESOURCE_TYPES`).

For more detailed steps, see Recording Resources (AWS CLI).

## Stopping AWS Config from recording with the customer managed configuration recorder

You can stop AWS Config from recording with the customer managed configuration recorder any time. After AWS Config stops recording a resource, it retains the configuration information that was previously captured, and you can continue to access this information.

For steps on how to stop recording, see Stopping the customer managed configuration recorder.

# Recording Configurations with AWS Config for Third-Party Resources using the AWS CLI

Record configurations for third-party resources or custom resource types such as on premise servers, SAAS monitoring tools, and version control systems (like GitHub).

You can publish the configuration data of third-party resources into AWS Config and view and monitor the resource inventory and configuration history using the AWS Config console and APIs. You can use AWS Config to manage all your resources and evaluate resource configuration for compliance against best practices using AWS Config rules. You can also create AWS Config rules or conformance packs to evaluate these third-party resources against best practices, internal policies, and regulatory policies.

> **Note**
>
> If you have configured AWS Config to record all resource types, then third-party resources that are managed (created, updated, or deleted) through CloudFormation are automatically tracked in AWS Config as configuration items.

**Prerequisite:** The third-party resources or custom resource type must be registered using CloudFormation.

**Topics**


- Adding Third-Party Resources to AWS Config
- Record Configuration Items with AWS Config for Third-Party Resources using the AWS CLI
- Read Configuration Items with AWS Config for Third-Party Resources using the AWS CLI
- Delete Third-Party Resources from AWS Config using the AWS CLI


## Adding Third-Party Resources to AWS Config

Follow these steps to add a third-party resource to AWS Config.

**Topics**


- Step 1: Setup Your Development Environment
- Step 2: Model Your Resource
- Step 3: Generate Artifacts
- Step 4: Register Your Resource
- Step 5: Publish Resource Configuration

## Step 1: Setup Your Development Environment

Install and configure the CloudFormation AWS CLI. The AWS CLI allows you to model and register your custom resources. For more information, see Custom Resources and What Is the CloudFormation Command Line Interface?.

## Step 2: Model Your Resource

Create a resource provider schema that conforms to and validates the configuration of the resource type.

1. Use the `init` command to create your resource provider project and generate the files it requires.

```
$ cfn init
Initializing new project
```

2. The `init` command launches a wizard that walks you through setting up the project, including specifying the resource name. For this walkthrough, specify `MyCustomNamespace::Testing::WordPress`.

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. Enter a package name for your resource.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> In order to guarantee that any project dependencies are correctly resolved, you can import the generated project into your IDE with Maven support.
> For example, if you are using IntelliJ IDEA, you would need to do the following:
>
> - From the **File** menu, choose **New**, then choose **Project From Existing Sources**.
> - Navigate to the project directory
> - In the **Import Project** dialog box, choose **Import project from external model** and then choose **Maven**.

- Choose **Next** and accept any defaults to complete importing the project.

4. Open the `mycustomnamespace-testing-wordpress.json` file that contains the schema for your resource. Copy and paste the following schema into `mycustomnamespace-testing-wordpress.json`.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Validate the schema.

```
$ cfn validate
```

6. Update the auto-generated files in the resource provider package to view the resource provider schema updates. Upon initiation of the resource provider project, the AWS CLI generates supporting files and code for the resource provider. Regenerate the code to see the updated schema.

```
$ cfn generate
```

> **Note**
>
> When using Maven, as part of the build process the `generate` command is automatically run before the code is compiled. So your changes will never get out of sync with the generated code.
> Be aware the CloudFormation CLI must be in a location Maven/the system can find. For more information, see Setting up your environment for developing extensions.

For more information on the whole process, see Modeling Resource Providers for Use in CloudFormation.

### Step 3: Generate Artifacts

Run the following command to generate artifacts for `cfn submit`.

```
$ mvn package
```

### Step 4: Register Your Resource

AWS Config does not require resource provider handlers to perform configuration tracking for your resource. Run the following command to register your resource.

```
$ cfn submit
```

For more information, see Registering Resource Providers for Use in CloudFormation Templates.

### Step 5: Publish Resource Configuration

Determine the configuration for MyCustomNamespace::Testing::WordPress.

```
{
```

```
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Determine the schema version id from CloudFormation `DescribeType`.

In AWS Config, you can see see if this resource configuration is accepted. To evaluate compliance you can write AWS Config rules using this resource.

(Optional) To automate recording of configuration, implement periodic or change-based configuration collectors.

## Record Configuration Items with AWS Config for Third-Party Resources using the AWS CLI

Record a configuration item for a third-party resource or a custom resource type using the following procedure:

Ensure you register the resource type `MyCustomNamespace::Testing::WordPress` with its matching schema.

1. Open a command prompt or a terminal window.
2. Enter the following command:

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> As defined in the type schema, `writeOnlyProperties` will be removed from the configuration prior to being recorded by AWS Config. This means that these values will not

be present when the configuration is obtained from read APIs. For more information on `writeOnlyProperties`, see Resource type schema.

## Read Configuration Items with AWS Config for Third-Party Resources using the AWS CLI

Read a configuration item for a third-party resource or a custom resource type using the following procedure:

1. Open a command prompt or a terminal window.
2. Enter the following command:

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Press Enter.

   You should see output similar to the following:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. Enter the following command:

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Press Enter.

   You should see output similar to the following:

```
{
    "unprocessedResourceKeys": [],
```

```
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

## Delete Third-Party Resources from AWS Config using the AWS CLI

Enter the following command to delete a third-party resource:

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

If successful, the command executes with no additional output.

# Recording Software Configuration for Managed Instances with AWS Config

You can use AWS Config to record software inventory changes on Amazon EC2 instances and on-premises servers. This enables you to see the historical changes to software configuration. For example, when a new Windows update is installed on a managed Windows instance, AWS Config records the changes and then sends the changes to your delivery channel, so that you are notified about the change. With AWS Config, you can see the history of when Windows updates were installed for the managed instance and how they changed over time.

### Topics

- Prerequisites

- Recording Software Configurations

## Prerequisites

You must complete the following steps to record software configuration changes:

- Turn on recording for the managed instance inventory resource type in AWS Config.
- Configure EC2 and on-premises servers as *managed instances* in AWS Systems Manager. A managed instance is a machine that has been configured for use with Systems Manager.
- Initiate collection of software inventory from your managed instances using the Systems Manager Inventory capability.

> **Note**
>
> **Systems Manager now supports creating configuration items for *unmanaged instances***
> Configuration item for unmanaged instances will have supplementary configuration with `Key: “InstanceStatus”` and `Value: “Unmanaged”`.
> **Configuration items for unmanaged instances won’t receive additional updates**
> To receive additional updates, the configuration item must be a managed instance.

You can also use AWS Config rules to monitor software configuration changes and be notified whether the changes are compliant or noncompliant against your rules. For example, if you create a rule that checks whether your managed instances have a specified application, and an instance doesn't have that application installed, AWS Config flags that instance as noncompliant against your rule. For a list of AWS Config managed rules, see List of AWS Config Managed Rules.

## Recording Software Configurations

**To enable recording of software configuration changes in AWS Config:**

1. Turn on recording for all supported resource types or selectively record the managed instance inventory resource type in AWS Config. For more information, see Recording AWS Resources with AWS Config.
2. Launch an Amazon EC2 instance with an instance profile for Systems Manager that includes the **AmazonSSMManagedInstanceCore** managed policy. This AWS managed policy enables an instance to use Systems Manager service core functionality.

For information about other policies you can add to the instance profile for Systems Manager, see Create an IAM Instance Profile for Systems Manager in the *AWS Systems Manager User Guide*.

> **Important**
>
> SSM Agent is Amazon software that must be installed on a managed instance in order to communicate with the Systems Manager in the cloud. If your EC2 instance was created from an AMI for one of the following operating systems, the agent is preinstalled:
>
> - Windows Server 2003-2012 R2 AMIs published in November 2016 or later
> - Windows Server 2016 and 2019
> - Amazon Linux
> - Amazon Linux 2
> - Ubuntu Server 16.04
> - Ubuntu Server 18.04
>
> On EC2 instances that were not created from an AMI with the agent preinstalled, you must install the agent manually. For information, see the following topics in the *AWS Systems Manager User Guide*:
>
> - Installing and configuring SSM Agent on EC2 instances for Windows Server
> - Installing and configuring SSM Agent on EC2 instances for Linux

3. Initiate inventory collection as described in Configuring Inventory Collection in the *AWS Systems Manager User Guide*. The procedures are the same for Linux and Windows instances.

   AWS Config can record configuration changes for the following inventory types:

   - **Applications** – A list of applications for managed instances, such as antivirus software.
   - **AWS components** – A list of AWS components for managed instances, such as the AWS CLI and SDKs.
   - **Instance information** – Instance information such as OS name and version, domain, and firewall status.

- **Network configuration** – Configuration information such as IP address, gateway, and subnet mask.
- **Windows Updates** – A list of Windows updates for managed instances (Windows instances only).

> **Note**
>
> AWS Config doesn't support recording the custom inventory type at this time.

Inventory collection is one of many Systems Manager capabilities, which are grouped in the categories *Operations Management*, *Actions & Change*, *Instances & Nodes*, and *Shared Resources*. For more information, see What is Systems Manager? and Systems Manager Capabilities in the *AWS Systems Manager User Guide*.

## Looking Up Resources That Are Discovered by AWS Config

You can use the AWS Config console, AWS CLI, and AWS Config API to look up the resources that AWS Config has taken an inventory of, or *discovered*, including deleted resources and resources that AWS Config is not currently recording. AWS Config discovers supported resource types only. For more information, see Supported Resource Types for AWS Config.

Looking Up Resources (Console)

You can use resource types or tag information to look up resources in the AWS Config console.

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. On the **Resource inventory** page, specify the search options for the resources that you want to look up:
   - **Resource category** – Choose all resource categories or narrow results to only AWS Resources.
   - **Resource type** – Choose all resource types or select which resource(s) to filter by.
   - **Compliance** – Choose to filter by any compliance status, compliant, or noncompliant.
3. AWS Config lists the resources that match your search options. You can see the following information about the resources:

- **Resource identifier** – The resource identifier might be a resource ID or a resource name, if applicable. Choose the resource identifier link to view the resource details page.
- **Resource type** – The type of the resource is listed.
- **Compliance** – The status of the resource that AWS Config evaluated against your rule.

### Looking Up Resources (AWS CLI)

You can use the AWS CLI to list resources that AWS Config has discovered.

Use the **AWS Configservice** `list-discovered-resources` command:

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

To view the configuration details of a resource that is listed in the response, use the `get-resource-config-history` command, and specify the resource type and ID. For an example of this command and the response from AWS Config, see Viewing Configuration History.

### Looking up Resources (API)

You specify a resource type, and AWS Config returns a list of resource identifiers for resources of that type. For more information, see ResourceIdentifier in the *AWS Config API Reference*.

Use the ListDiscoveredResources action.

To get the configuration details of a resource that is listed in the response, use the GetResourceConfigHistory action, and specify the resource type and ID.

# Viewing Compliance Information and Evaluation Results for your AWS Resources with AWS Config

> **Important**
>
> For accurate reporting on the compliance status, you must record the `AWS::Config::ResourceCompliance` resource type. For more information, see Recording AWS Resources.

You can use the AWS Config console or AWS SDKs to view the compliance information and the evaluation results of your resources.

**Topics**


- Viewing compliance (Console)
- Viewing compliance (AWS SDKs)


## Viewing compliance (Console)

**To view compliance (Console)**

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Resources**. On the Resource inventory page, you can filter by resource category, resource type, and compliance status. Choose **Include deleted resources** if appropriate. The table displays the resource identifier for the resource type and the resource compliance status for that resource. The resource identifier might be a resource ID or a resource name.
4. Choose a resource from the resource identifier column.
5. Choose the **Resource Timeline** button. You can filter by Configuration events, Compliance events, or CloudTrail Events.

> **Note**
>
> Alternatively, on the Resource inventory page, you can directly choose the resource name. To access the resource timeline from the resource details page, choose the **Resource Timeline** button.

You can also view the compliance of your resources by looking them up on the **Resource inventory** page. For more information, see Looking Up Resources That Are Discovered by AWS Config.

## Viewing compliance (AWS SDKs)

**To get compliance information for your AWS resources**

The following code examples show how to use `DescribeComplianceByResource`.

CLI

**AWS CLI**

**To get compliance information for your AWS resources**

The following command returns compliance information for each EC2 instance that is recorded by AWS Config and that violates one or more rules:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many rules the resource violates. For example, the following output indicates that instance `i-1a2b3c4d` violates 2 rules.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
```

```
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- For API details, see DescribeComplianceByResource in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.**

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

**Output:**

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.**

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

**Output:**

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

### To get the compliance summary of your AWS resources

The following code examples show how to use `GetComplianceSummaryByResourceType`.

CLI

**AWS CLI**

**To get the compliance summary for all resource types**

The following command returns the number of AWS resources that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type
```

In the output, the value for each `CappedCount` attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

**To get the compliance summary for a specific resource type**

The following command returns the number of EC2 instances that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

In the output, the value for each `CappedCount` attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
```

```
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- For API details, see GetComplianceSummaryByResourceType in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.**

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.**

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
```

```
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

### To get the evaluation results for an AWS resource

The following code examples show how to use `GetComplianceDetailsByResource`.

CLI

#### AWS CLI

##### To get the evaluation results for an AWS resource

The following command returns the evaluation results for each rule with which the EC2 instance `i-1a2b3c4d` does not comply:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
```

```
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- For API details, see GetComplianceDetailsByResource in *AWS CLI Command Reference*.

PowerShell

### Tools for PowerShell V4

#### Example 1: This example evaulation results for the given resource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

#### Output:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- For API details, see GetComplianceDetailsByResource in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example evaulation results for the given resource.**

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

**Output:**

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- For API details, see GetComplianceDetailsByResource in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

# Viewing Compliance History for your AWS Resources with AWS Config

> **Important**
>
> The `AWS::Config::ResourceCompliance` resource type is used to store historical compliance results for resources. Recording this resource type is **not required** for Config rules to evaluate resources or for viewing current compliance status in the console. Recording `AWS::Config::ResourceCompliance` only enables you to view historical compliance changes over time in the resource timeline. If you don't need historical compliance data, you can exclude this resource type. For more information about selecting resources to record, see Recording AWS Resources.

You can view the configuration, relationships, and number of changes made to a resource in the AWS Config console. You can view the configuration history for a resource using AWS CLI.

**Topics**


- Viewing Compliance History (Console)
- Viewing Compliance History (AWS CLI)
- Viewing Compliance History Timeline for Resources and Rules


## Viewing Compliance History (Console)

### Viewing Compliance History Using the Console

When you look up resources on the **Resource inventory** page, choose the resource name or ID in the resource identifier column to view the resource's details page. The details page provides information about the configuration, relationships, and number of changes made to that resource.

To access the resource timeline from the resource details page, choose the **Resource Timeline** button. The Resource timeline captures changes as `ConfigurationItems` over a period of time for a specific resource. You can filter by Configuration events, Compliance events, or CloudTrail Events.

## Viewing Compliance History (AWS CLI)

### Viewing Compliance History Using the AWS CLI

The configuration items that AWS Config records are delivered to the specified delivery channel on demand as a configuration snapshot and as a configuration stream. You can use the AWS CLI to view history of configuration items for each resource.

### Viewing Configuration History

Enter the `get-resource-config-history` command and specify the resource type and the resource ID, for example:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
```

```
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
```

```
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

For detailed explanation of the response fields, see Components of a Configuration Item and Supported Resource Types for AWS Config.

**Example Amazon EBS Configuration History from AWS Config**

AWS Config generates a set of files that each represent a resource type and lists all configuration changes for the resources of that type that AWS Config is recording. AWS Config exports this resource-centric configuration history as an object in the Amazon S3 bucket that you specified when you enabled AWS Config. The configuration history file for each resource type contains the changes that were detected for the resources of that type since the last history file was delivered. The history files are typically delivered every six hours.

The following is an example of the contents of the Amazon S3 object that describes the configuration history of all the Amazon Elastic Block Store volumes in the current region for your AWS account. The volumes in this account include `vol-ce676ccc` and `vol-cia007c`. Volume `vol-ce676ccc` had two configuration changes since the previous history file was delivered while volume `vol-cia007c` had one change.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
```

```
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
```

```
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
```

```
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
```

```
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

## Viewing Compliance History Timeline for Resources and Rules

AWS Config supports storing compliance state changes of resources as evaluated by AWS Config Rules. The resource compliance history is presented in the form of a timeline. The timeline captures changes as `ConfigurationItems` over a period of time for a specific resource. For information on the contents of `ConfigurationItem`, see ConfigurationItem in the AWS Config API Reference.

You can opt in or out to record all resource types in AWS Config. If you have opted to record all resource types, AWS Config automatically begins recording the resource compliance history as evaluated by AWS Config Rules. By default, AWS Config records the configuration changes for all supported resources. You can also select only the specific resource compliance history resource type: `AWS::Config::ResourceCompliance`. For more information, see Recording AWS Records.

Viewing Resource Timeline Using Resources

Access the resource timeline by selecting a specific resource from the Resource inventory page.

1. Choose the **Resources** from the left navigation.
2. On the Resource inventory page, you can filter by resource category, resource type, and compliance status. Choose **Include deleted resources** if appropriate.

   The table displays the resource identifier for the resource type and the resource compliance status for that resource. The resource identifier might be a resource ID or a resource name.
3. Choose a resource from the resource identifier column.

4. Choose the **Resource Timeline** button. You can filter by Configuration events, Compliance events, or CloudTrail Events.

> **Note**
>
> Alternatively, on the Resource inventory page, you can directly choose the resource name. To access the resource timeline from the resource details page, choose the **Resource Timeline** button.

Viewing Resource Timeline Using Rules

Access the resource timeline by selecting a specific rule from the Rule page.

1. Select the **Rules** from the left navigation.
2. On the Rule page, choose a rule evaluating your relevant resources. If no rules are displayed on the screen, add rules using the **Add rule** button.
3. On the Rule details page, select the resources from the Resources evaluated table.
4. Select the **Resource Timeline** button. The resource timeline is displayed.

# Querying Compliance History for your AWS Resources

Query the resource compliance history using get-resource-config-history using the resource type `AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

You should see output similar to the following:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
```

```
      "relationshipName": "Is associated with "
     }
    ]
    "tags": {},
    "resourceType": "AWS::Config::ResourceCompliance",
    "resourceId": "AWS::S3::Bucket/configrules-bucket",
    "ConfigurationStateId": "1539799966921",
    "relatedEvents": [];
    "awsRegion": "us-west-2",
    "version": "1.3",
    "configurationItemMD5Hash": "",
    "supplementaryConfiguration": {},
    "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "AccountID"
   }
  ]
}
```

# Tagging Your AWS Config Resources

A tag is a label that you assign to an AWS resource. Each tag consists of a *key* and an optional *value*, both of which you define. Tags make it easier to manage, search for, and filter resources.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags you've assigned to it. You can assign one or more tags to your AWS resources. Each tag has an associated value.

We recommend that you devise a set of tag keys that meets your needs for each resource type. Using a consistent set of tag keys makes it easier for you to manage your AWS resources. You can search and filter the resources based on the tags you add.

Tags are interpreted strictly as a string of characters and are not automatically assigned to your resources. You can edit tag keys and values, and you can remove tags from a resource at any time. You can set the value of a tag to an empty string, but you can't set the value of a tag to null. If you

add a tag that has the same key as an existing tag on that resource, the new value overwrites the old value. If you delete a resource, any tags for the resource are also deleted.

You can work with tags using the AWS Command Line Interface (AWS CLI) and the AWS Config API reference.

## Restrictions Related to Tagging

The following basic restrictions apply to tags.

| Restriction | Description |
| --- | --- |
| Maximum number of tags per resource | 50 |
| Maximum key length | 128 Unicode characters in UTF-8 |
| Maximum value length | 256 Unicode characters in UTF-8 |
| Prefix restriction | Do not use the `aws:` prefix in your tag names or values because it is reserved for AWS use. You can't edit or delete tag names or values with this prefix. Tags with this prefix do not count against your tags per resource limit. |
| Character restrictions | Tags may only contain Unicode letters, digits, whitespace, or these symbols: `_ . : / = + - @` |

## Managing Tags with AWS Config API Actions

Tag based access controls are available for three resources `ConfigurationAggregator`, `AggregationAuthorization`, and `ConfigRule`. Use the following to add, update, list, and delete the tags for your resources.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource` and `UntagResource` require certain AWS Identity and Access Management (IAM) permissions to control access. For more information, see Controlling access based on tag keys in the IAM User Guide.

# Evaluating Resources with AWS Config Rules

Use AWS Config to evaluate the configuration settings of your AWS resources. You do this by creating AWS Config rules, which represent your ideal configuration settings. AWS Config provides customizable, predefined rules called managed rules to help you get started.

**Topics**


- Considerations
- Region Support
- Components of an AWS Config Rule
- AWS Config Managed Rules
- AWS Config Custom Rules
- Service-Linked AWS Config Rules
- Managing AWS Config Rules Across All Accounts in Your Organization
- Adding AWS Config Rules
- Updating AWS Config Rules
- Deleting AWS Config Rules
- Viewing Details and Compliance Information for your AWS Config Rules
- Turning on Proactive Evaluation for AWS Config Rules
- Sending Rule Evaluations to Security Hub CSPM
- Evaluating Your Resources with AWS Config Rules
- Deleting Evaluation Results from AWS Config Rules
- Troubleshooting for AWS Config rules


## Considerations

Cost Considerations

For details about the costs associated with resource recording, see AWS Config pricing.

**Recommendation: Consider excluding the `AWS::Config::ResourceCompliance` resource type from recording before deleting rules**

Deleting rules creates configuration items (CIs) for `AWS::Config::ResourceCompliance` that can affect your costs for the configuration recorder. If you are deleting rules which evaluate a large number of resource types, this can lead to a spike in the number of CIs recorded.

To avoid the associated costs, you can opt to disable recording for the `AWS::Config::ResourceCompliance` resource type before deleting rules, and re-enable recording after the rules have been deleted.

However, since deleting rules is an asynchronous process, it might take an hour or more to complete. During the time when recording is disabled for `AWS::Config::ResourceCompliance`, rule evaluations will not be recorded in the associated resource's history.

AWS Config recommends that you weigh these factors on a case-by-case basis before deciding how to proceed with deleting rules.

**Recommendation: Add logic to handle the evaluation of deleted resources for custom lambda rules**

When creating AWS Config custom lambda rules, it is highly recommended that you add logic to handle the evaluation of deleted resources.

When evaluation results are marked as `NOT_APPLICABLE`, they will be marked for deletion and cleaned up. If they're NOT marked as `NOT_APPLICABLE`, the evaluation results will remain unchanged until the rule is deleted, which can cause an unexpected spike in the creation of CIs for `AWS::Config::ResourceCompliance` upon rule deletion.

For information on how to set AWS Config custom lambda rules to return `NOT_APPLICABLE` for deleted resources, see Managing deleted resources with AWS Config custom lambda rules.

**Recommendation: Provide the resources in scope for custom lambda rules**

AWS Config Custom Lambda Rules can cause a high number of Lambda function invocations if the rule is not scoped to one or more resource types. To avoid increased activity associated with your account, it is highly recommended to provide resources in scope for your Custom Lambda rules. If no resource types are selected, the rule will invoke the Lambda function for all resources in the account.

Other considerations

**Defaut Values for Managed Rules**

The default values specified for managed rules are pre-populated only when using the AWS console. Default values are not supplied for the API, CLI, or SDK.

**Configuration Item Recording Delays**

AWS Config usually records configuration changes to your resources right after a change is detected, or at the frequency that you specify. However, this is on a best effort basis and can take longer at times. For example, a resource type with known delays is `AWS::SecretsManager::Secret`. This resource type is an example, and this list is non-exhaustive.

**Policies and compliance results**

IAM policies and other policies managed in AWS Organizations can impact whether AWS Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use AWS Config.

**Tagging support for resource types**

If a resource type does not support tagging or does not include tag information in its describe API response, AWS Config won't capture tag data in the configuration items (CIs) for that resource type. AWS Config will still record these resources. However, any functionality that relies on tag data won't work. This affects tag-based filtering, grouping, or compliance evaluation that relies on tag data.

**Directory Buckets Are Not Supported**

Managed rules only support general purpose buckets when evaluating Amazon Simple Storage Service (Amazon S3) resources. For more information on general purpose buckets and directory buckets, see Buckets overview and Directory buckets in the Amazon S3 User Guide.

**Managed Rules and Global IAM Resource Types**

The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.

If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.

To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

## Region Support

Currently, the AWS Config Rule feature is supported in the following AWS regions. For a list of which individual AWS Config rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com<br>config-fips.us-east-2.amazonaws.com | HTTPS<br>HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com<br>config-fips.us-east-1.amazonaws.com | HTTPS<br>HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com<br>config-fips.us-west-1.amazonaws.com | HTTPS<br>HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com<br>config-fips.us-west-2.amazonaws.com | HTTPS<br>HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS | |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS | |
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS | |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS | |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS | |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS | |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS | |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS |
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

Deploying AWS Config Rules across member accounts in an AWS Organization is supported in the following Regions.

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# Components of an AWS Config Rule

AWS Config rules evaluate the configuration settings of your AWS resources. This page discusses the components of a rule.

**Topics**


- How AWS Config Rules Work
- Trigger Types
- Evaluation Modes
- AWS Config Rule Metadata


## How AWS Config Rules Work

While AWS Config continuously tracks the configuration changes that occur among your resources, it checks whether these changes do not comply with the conditions in your rules. If a resource does not comply with rule, AWS Config flags the resource and the rule as *noncompliant*.

There are four possible evaluation results for an AWS Config rule.

| Evaluation result | Description |
| --- | --- |
| `COMPLIANT` | The rule passes the conditions of the compliance check. |
| `NON_COMPLIANT` | The rule fails the conditions of the compliance check. |
| `ERROR` | The one of the required/optional parameter s is not valid, not of the correct type, or is formatted incorrectly. |
| `NOT_APPLICABLE` | Used to filter out resources that the logic of the rule cannot be applied to. For example, the alb-desync-mode-check rule only checks Application Load Balancers, and ignores Network Load Balancers and Gateway Load Balancers. |

For example, when an EC2 volume is created, AWS Config can evaluate the volume against a rule that requires volumes to be encrypted. If the volume is not encrypted, AWS Config flags the volume and the rule as noncompliant. AWS Config can also check all of your resources for account-wide requirements. For example, AWS Config can check whether the number of EC2 volumes in an account stays within a desired total, or whether an account uses AWS CloudTrail for logging.

## Trigger Types

After you add a rule to your account, AWS Config compares your resources to the conditions of the rule. After this initial evaluation, AWS Config continues to run evaluations each time one is triggered. The evaluation triggers are defined as part of the rule, and they can include the following types.

| Trigger type | Description |
| --- | --- |
| Configuration changes | AWS Config runs evaluations for the rule when there is a resource that matches the rule's scope and there is a change in configuration of the resource. The evaluation runs after AWS Config sends a configuration item change notification.<br><br>You choose which resources initiate the evaluation by defining the rule's *scope*. The scope can include the following:<br><br>• One or more resource types<br>• A combination of a resource type and a resource ID<br>• A combination of a tag key and value<br>• When any recorded resource is created, updated, or deleted<br><br>AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to define which resources initiate evaluations. |

| Trigger type | Description |
| --- | --- |
| Periodic | AWS Config runs evaluations for the rule at a frequency that you choose; for example, every 24 hours. |
| Hybrid | Some rules have both configuration change and periodic triggers. For these rules, AWS Config evaluates your resources when it detects a configuration change and also at the frequency that you specify. |

## Evaluation Modes

There are two evaluation modes for AWS Config rules.

| Evaluation mode | Description |
| --- | --- |
| Proactive | Use proactive evaluation to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region. |
| Detective | Use detective evaluation to evaluate resources that have already been deployed. This allows you to evaluate the configuration settings of your existing resources. |

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

For more information, see Turning on Proactive Evaluation for AWS Config Rules.

### List of managed rules with proactive evaluation

For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.

### List of supported resource types for proactive evaluation

The following is a list of resource types that are supported for proactive evaluation:

- `AWS::EC2::EIP`

## AWS Config Rule Metadata

AWS Config rules can contain the following mutable metadata:

**defaultName**

The defaultName is the name that instances of a rule will get by default.

**description**

The rule description provides context for what the rule evaluates. The AWS Config Console has a limit of 256 characters. As a best practice, the rule description should begin with “Checks if” and include a description of the NON_COMPLIANT scenario. Service Names should be written in full beginning with AWS or Amazon when first mentioned in the rule description. For example, AWS CloudTrail or Amazon CloudWatch instead of CloudTrail or CloudWatch for first use. Services names can be abbreviated after subsequent reference.

**scope**

The scope determines which resource types the rule targets. For a list of supported resource types, see Supported Resource Types.

**compulsoryInputParameterDetails**

The compulsoryInputParameterDetails are used for parameters that are required for a rule to do its evaluation. For example, the `access-keys-rotated` managed rule includes `maxAccessKeyAge` as a required parameter. If a parameter is required, it will not be marked as (Optional). For each parameter, a type must be specified. Type can be one of "String", "int", "double", "CSV", "boolean" and "StringMap".

**optionalInputParameterDetails**

The optionalInputParameterDetails are used for parameters that are optional for a rule to do its evaluation. For example, the `elasticsearch-logs-to-cloudwatch` managed rule includes `logTypes` as an optional parameter. For each parameter, a type must be specified. Type can be one of "String", "int", "double", "CSV", "boolean" and "StringMap".

**supportedEvaluationModes**

The supportedEvaluationModes determines when resources will be evaluated, either before a resource has been deployed or after a resource has been deployed.

`DETECTIVE` is used to evaluate resources which have already been deployed. This allows you to evaluate the configuration settings of your existing resources. `PROACTIVE` is used to evaluate resources before they have been deployed.

This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

You can specify the supportedEvaluationModes to `DETECTIVE`, `PROACTIVE`, or both `DETECTIVE` and `PROACTIVE`. You must specify an evaluation mode and this field cannot remain empty.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

# AWS Config Managed Rules

AWS Config provides *AWS managed rules*, which are predefined, customizable rules that AWS Config uses to evaluate whether your AWS resources comply with common best practices. For example, you could use a managed rule to quickly start assessing whether your Amazon Elastic Block Store (Amazon EBS) volumes are encrypted or whether specific tags are applied to your resources.

The AWS Config console guides you through the process of configuring and activating a managed rule. You can also use the AWS Command Line Interface or AWS Config API to pass the JSON code that defines your configuration of a managed rule.

You can customize the behavior of a managed rule to suit your needs. For example, you can define the rule's scope to constrain which resources trigger an evaluation for the rule, such as EC2 instances or volumes.

You can customize the rule's parameters to define attributes that your resources must have to comply with the rule. For example, you can customize a parameter to specify that your security group should block incoming traffic to a specific port number.

Before using managed rules, see Considerations.

**Topics**


- List of AWS Config Managed Rules
- List of AWS Config Managed Rules by Evaluation Mode
- List of AWS Config Managed Rules by Trigger Type
- List of AWS Config Managed Rules by Region Availability
- Creating AWS Config Managed Rules With AWS CloudFormation Templates


## List of AWS Config Managed Rules

AWS Config currently supports the following managed rules. Before using these rules, see Considerations.

**Topics**


- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged

- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target

- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-distribution-key-group-enabled
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-oac-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled

- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled

- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled

- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted

- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged

- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check

- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- route53-health-check-tagged
- route53-hosted-zone-tagged
- route53-query-logging-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## access-keys-rotated

Checks if active IAM access keys are rotated (changed) within the number of days specified in `maxAccessKeyAge`. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days.

> **Warning**
>
> Do not provide your access keys to unauthorized parties, even to help find your account identifiers. By doing this, you might give someone permanent access to your account. The security best practice is to remove passwords and access keys when users no longer need them.

> **Note**
>
> **Resource Type Marked as Noncompliant in the Console**
> If this rule finds that any of your access keys are noncompliant, the `AWS::IAM::User` resource type will also be marked as noncompliant in the AWS console.
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.
> **Limitations**
> This rule does not apply to AWS account root user access keys. To delete or rotate your root user access keys, use your root user credentials to sign in to the My Security Credentials page in the AWS Management Console at https://aws.amazon.com/console/.

**Identifier:** ACCESS_KEYS_ROTATED

**Resource Types:** AWS::IAM::User

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

maxAccessKeyAge, Type: int, Default: 90

Maximum number of days without rotation. Default 90.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### account-part-of-organizations

Checks if an AWS account is part of AWS Organizations. The rule is NON_COMPLIANT if an AWS account is not part of AWS Organizations or AWS Organizations master account ID does not match rule parameter `MasterAccountId`.

> **Note**
>
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.

To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** ACCOUNT_PART_OF_ORGANIZATIONS

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing) Region

**Parameters:**

MasterAccountId (Optional), Type: String

The master account ID for an AWS account.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## acmpca-certificate-authority-tagged

Checks if AWS Private CA certificate authorities have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ACMPCA_CERTIFICATE_AUTHORITY_TAGGED

**Resource Types:** AWS::ACMPCA::CertificateAuthority

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### acm-certificate-expiration-check

Checks if AWS Certificate Manager Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed. ACM does not automatically renew certificates that you import. The rule is NON_COMPLIANT if your certificates are about to expire.

**Identifier:** ACM_CERTIFICATE_EXPIRATION_CHECK

**Resource Types:** AWS::ACM::Certificate

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

daysToExpiration (Optional), Type: int, Default: 14

Specify the number of days before the rule flags the ACM Certificate as noncompliant.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### acm-certificate-rsa-check

Checks if RSA certificates managed by AWS Certificate Manager (ACM) have a key length of at least '2048' bits.The rule is NON_COMPLIANT if the minimum key length is less than 2048 bits.

**Identifier:** ACM_CERTIFICATE_RSA_CHECK

**Resource Types:** AWS::ACM::Certificate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## acm-pca-root-ca-disabled

Checks if AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED.

**Identifier:** ACM_PCA_ROOT_CA_DISABLED

**Resource Types:** AWS::ACMPCA::CertificateAuthority

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

exemptedCAArns (Optional), Type: CSV

Comma-separated list of Amazon Resource Names (ARN) of CA's that can be enabled. This value can be supplied for other CAs, like specific root CAs or intermediate CA's that can be enabled.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## active-mq-supported-version

Checks if an Amazon MQ ActiveMQ broker is running on a specified minimum supported engine version. The rule is NON_COMPLIANT if the ActiveMQ broker is not running on the minimum supported engine version that you specify.

**Identifier:** ACTIVE_MQ_SUPPORTED_VERSION

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

supportedEngineVersion, Type: String

> String value for the rule to check the minimum supported engine version for the ActiveMQ broker. ActiveMQ brokers use semantic versioning specification: X.Y.Z. X denotes the major version, Y represents the minor version, and Z denotes the patch version.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## alb-desync-mode-check

Checks if an Application Load Balancer (ALB) is configured with a user defined desync mitigation mode. The rule is NON_COMPLIANT if ALB desync mitigation mode does not match with the user defined desync mitigation mode.

**Identifier:** ALB_DESYNC_MODE_CHECK

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

desyncMode, Type: CSV

Comma-separated list, in which customers can choose max 2 values among - 'defensive', 'strictest', and 'monitor'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## alb-http-drop-invalid-header-enabled

Checks if rule evaluates AWS Application Load Balancers (ALB) to ensure they are configured to drop http headers. The rule is NON_COMPLIANT if the value of routing.http.drop_invalid_header_fields.enabled is set to false

**Identifier:** ALB_HTTP_DROP_INVALID_HEADER_ENABLED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## alb-http-to-https-redirection-check

Checks if HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers. The rule is NON_COMPLIANT if one or more HTTP listeners of Application Load Balancer do not have HTTP to HTTPS redirection configured. The rule is also NON_COMPLIANT if one of more HTTP listeners have forwarding to an HTTP listener instead of redirection.

**Identifier:** ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## alb-internal-scheme-check

Checks if an Application Load Balancer scheme is internal. The rule is NON_COMPLIANT if configuration.scheme is not set to internal.

**Identifier:** ALB_INTERNAL_SCHEME_CHECK

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## alb-listener-tagged

Checks if Application Load Balancer listeners have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ALB_LISTENER_TAGGED

**Resource Types:** AWS::ElasticLoadBalancingV2::Listener

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## alb-tagged

Checks if Application Load Balancers have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ALB_TAGGED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## alb-waf-enabled

Checks if Web Application Firewall (WAF) is enabled on Application Load Balancers (ALBs). This rule is NON_COMPLIANT if key: waf.enabled is set to false.

**Identifier:** ALB_WAF_ENABLED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

wafWebAclIds (Optional), Type: CSV

Comma separated list of web ACL ID (for WAF) or web ACL ARN (for WAFV2) checking for ALB association

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## amplify-app-branch-auto-deletion-enabled

Checks if AWS Amplify apps automatically disconnect a branch in Amplify Hosting when you delete a branch from your Git repository. The rule is NON_COMPLIANT if configuration.EnableBranchAutoDeletion is false.

**Identifier:** AMPLIFY_APP_BRANCH_AUTO_DELETION_ENABLED

**Resource Types:** AWS::Amplify::App

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## amplify-app-description

Checks if AWS Amplify apps have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** AMPLIFY_APP_DESCRIPTION

**Resource Types:** AWS::Amplify::App

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## amplify-app-no-environment-variables

Checks that AWS Amplify apps do not contain environment variables. The rule is NON_COMPLIANT if configuration.EnvironmentVariables is not an empty list.

**Identifier:** AMPLIFY_APP_NO_ENVIRONMENT_VARIABLES

**Resource Types:** AWS::Amplify::App

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## amplify-app-tagged

Checks if AWS Amplify apps have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** AMPLIFY_APP_TAGGED

**Resource Types:** AWS::Amplify::App

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### amplify-branch-description

Checks if AWS Amplify branches have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** AMPLIFY_BRANCH_DESCRIPTION

**Resource Types:** AWS::Amplify::Branch

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### amplify-branch-performance-mode-enabled

Checks if AWS Amplify branches have performance mode enabled. The rule is NON_COMPLIANT if configuration.EnablePerformanceMode is false.

**Identifier:** AMPLIFY_BRANCH_PERFORMANCE_MODE_ENABLED

**Resource Types:** AWS::Amplify::Branch

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## amplify-branch-tagged

Checks if AWS Amplify branches have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** AMPLIFY_BRANCH_TAGGED

**Resource Types:** AWS::Amplify::Branch

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### apigatewayv2-stage-description

Checks if Amazon API Gateway V2 stages have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** APIGATEWAYV2_STAGE_DESCRIPTION

**Resource Types:** AWS::ApiGatewayV2::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### apigateway-stage-access-logs-enabled

Checks if Amazon API Gateway stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration.

**Identifier:** APIGATEWAY_STAGE_ACCESS_LOGS_ENABLED

**Resource Types:** AWS::ApiGateway::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apigateway-stage-description

Checks if Amazon API Gateway stages have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** APIGATEWAY_STAGE_DESCRIPTION

**Resource Types:** AWS::ApiGateway::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gwv2-access-logs-enabled

Checks if Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration.

**Identifier:** API_GWV2_ACCESS_LOGS_ENABLED

**Resource Types:** AWS::ApiGatewayV2::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gwv2-authorization-type-configured

Checks if Amazon API Gatewayv2 API routes have an authorization type set. This rule is NON_COMPLIANT if the authorization type is NONE.

**Identifier:** API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

**Resource Types:** AWS::ApiGatewayV2::Route

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

authorizationType (Optional), Type: String

Parameter to check API routes' authorization types against. String parameters matching CUSTOM, AWS_IAM, JWT are valid.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gwv2-stage-default-route-detailed-metrics-enabled

Checks if the default route settings for Amazon API Gateway V2 stages have detailed metrics enabled. The rule is NON_COMPLIANT if configuration.defaultRouteSettings.detailedMetricsEnabled is false.

**Identifier:** API_GWV2_STAGE_DEFAULT_ROUTE_DETAILED_METRICS_ENABLED

**Resource Types:** AWS::ApiGatewayV2::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-associated-with-waf

Checks if an Amazon API Gateway API stage is using an AWS WAF web access control list (web ACL). The rule is NON_COMPLIANT if an AWS WAF Web ACL is not used or if a used AWS Web ACL does not match what is listed in the rule parameter.

**Identifier:** API_GW_ASSOCIATED_WITH_WAF

**Resource Types:** AWS::ApiGateway::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

WebAclArns (Optional), Type: CSV

Comma-separated list of web ACL Amazon Resource Names (ARNs)

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-cache-enabled-and-encrypted

Checks if all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in an Amazon API Gateway stage is not configured to cache or the cache is not encrypted.

**Identifier:** API_GW_CACHE_ENABLED_AND_ENCRYPTED

**Resource Types:** AWS::ApiGateway::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-endpoint-type-check

Checks if Amazon API Gateway APIs are of the type specified in the rule parameter `endpointConfigurationType`. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter.

**Identifier:** API_GW_ENDPOINT_TYPE_CHECK

**Resource Types:** AWS::ApiGateway::RestApi

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

endpointConfigurationTypes, Type: CSV

> Comma-separated list of allowed endpointConfigurationTypes. Allowed values are REGIONAL, PRIVATE and EDGE.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-execution-logging-enabled

Checks if all methods in Amazon API Gateway stages have logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or if `loggingLevel` is neither ERROR nor INFO.

**Identifier:** API_GW_EXECUTION_LOGGING_ENABLED

**Resource Types:** AWS::ApiGateway::Stage, AWS::ApiGatewayV2::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

loggingLevel (Optional), Type: String, Default: ERROR,INFO

Comma-separated list of specific logging levels (for example, ERROR, INFO or ERROR,INFO).

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-rest-api-tagged

Checks if AWS ApiGateway REST API resources resources have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** API_GW_REST_API_TAGGED

**Resource Types:** AWS::ApiGateway::RestApi

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-ssl-enabled

Checks if a REST API stage uses an SSL certificate. The rule is NON_COMPLIANT if the REST API stage does not have an associated SSL certificate.

> **Note**
>
> This rule returns `NOT_APPLICABLE` if the GetIntegration API returns `AWS` as type.

**Identifier:** API_GW_SSL_ENABLED

**Resource Types:** AWS::ApiGateway::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

CertificateIDs (Optional), Type: CSV

Comma-separated list of client certificate IDs configured on a REST API stage.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-stage-tagged

Checks if AWS ApiGateway stage resources resources have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** API_GW_STAGE_TAGGED

**Resource Types:** AWS::ApiGateway::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## api-gw-xray-enabled

Checks if AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise.

**Identifier:** API_GW_XRAY_ENABLED

**Resource Types:** AWS::ApiGateway::Stage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-application-description

Checks if AWS AppConfig applications have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** APPCONFIG_APPLICATION_DESCRIPTION

**Resource Types:** AWS::AppConfig::Application

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-application-tagged

Checks if AWS AppConfig applications have tags. Optionally, you can specify tag keys for the rule to check. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPCONFIG_APPLICATION_TAGGED

**Resource Types:** AWS::AppConfig::Application

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-configuration-profile-tagged

Checks if AWS AppConfig configuration profiles have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPCONFIG_CONFIGURATION_PROFILE_TAGGED

**Resource Types:** AWS::AppConfig::ConfigurationProfile

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-configuration-profile-validators-not-empty

Checks if an AWS AppConfig configuration profile includes at least one validator for syntactic or semantic check to ensure the configuration deploy functions as intended. The rule is NON_COMPLIANT if the Validators property is an empty array.

**Identifier:** APPCONFIG_CONFIGURATION_PROFILE_VALIDATORS_NOT_EMPTY

**Resource Types:** AWS::AppConfig::ConfigurationProfile

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-deployment-strategy-description

Checks if AWS AppConfig deployment strategies have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** APPCONFIG_DEPLOYMENT_STRATEGY_DESCRIPTION

**Resource Types:** AWS::AppConfig::DeploymentStrategy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-deployment-strategy-minimum-final-bake-time

Checks if an AWS AppConfig deployment strategy requires the specified minimum bake time. The rule is NON_COMPLIANT if the deployment strategy has a final bake time less than value specified in the rule parameter. The default value is 30 minutes.

**Identifier:** APPCONFIG_DEPLOYMENT_STRATEGY_MINIMUM_FINAL_BAKE_TIME

**Resource Types:** AWS::AppConfig::DeploymentStrategy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

minBakeTime (Optional), Type: int, Default: 30

The minimum bake time in minutes of the AWS AppConfig deployment strategy for the rule to check. The rule is NON_COMPLIANT if the bake time is less than the value specified in this parameter. Valid values are 0 to 1440. The default value is 30.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-deployment-strategy-replicate-to-ssm

Checks if AWS AppConfig deployment strategies save the deployment strategy to an AWS Systems Manager (SSM) document. The rule is NON_COMPLIANT if configuration.ReplicateTo is not 'SSM_DOCUMENT'.

**Identifier:** APPCONFIG_DEPLOYMENT_STRATEGY_REPLICATE_TO_SSM

**Resource Types:** AWS::AppConfig::DeploymentStrategy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-deployment-strategy-tagged

Checks if AWS AppConfig deployment strategies have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPCONFIG_DEPLOYMENT_STRATEGY_TAGGED

**Resource Types:** AWS::AppConfig::DeploymentStrategy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

includePredefinedSystemResources, Type: boolean, Default: False

A boolean that specifies whether to include predefined deployment strategies for the rule to check. The default value is false.

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-environment-description

Checks if AWS AppConfig environments have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** APPCONFIG_ENVIRONMENT_DESCRIPTION

**Resource Types:** AWS::AppConfig::Environment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-environment-tagged

Checks if AWS AppConfig environments have tags. Optionally, you can specify tag keys for the rule to check. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPCONFIG_ENVIRONMENT_TAGGED

**Resource Types:** AWS::AppConfig::Environment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-extension-association-tagged

Checks if AWS AppConfig extension associations have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPCONFIG_EXTENSION_ASSOCIATION_TAGGED

**Resource Types:** AWS::AppConfig::ExtensionAssociation

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-freeform-profile-config-storage

Checks if freeform configuration profiles for AWS AppConfig store their configuration data in AWS Secrets Manager or AWS AppConfig hosted configuration store. The rule is NON_COMPLIANT if configuration.LocationUri is not secretsmanager or hosted.

**Identifier:** APPCONFIG_FREEFORM_PROFILE_CONFIG_STORAGE

**Resource Types:** AWS::AppConfig::ConfigurationProfile

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appconfig-hosted-configuration-version-description

Checks if AWS AppConfig hosted configuration versions have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** APPCONFIG_HOSTED_CONFIGURATION_VERSION_DESCRIPTION

**Resource Types:** AWS::AppConfig::HostedConfigurationVersion

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud

(US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appflow-flow-tagged

Checks if Amazon AppFlow flows have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPFLOW_FLOW_TAGGED

**Resource Types:** AWS::AppFlow::Flow

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Africa (Cape Town), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appflow-flow-trigger-type-check

Checks if an Amazon AppFlow flow runs using the specified trigger type. The rule is NON_COMPLAINT if the flow does not run using the flow type specified in the required rule parameter.

**Identifier:** APPFLOW_FLOW_TRIGGER_TYPE_CHECK

**Resource Types:** AWS::AppFlow::Flow

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Africa (Cape Town), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

triggerType, Type: CSV

> Comma-separated list of trigger types for the rule to check. Valid values include: 'Scheduled', 'Event', and 'OnDemand'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appintegrations-event-integration-description

Checks if Amazon AppIntegrations event integrations have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** APPINTEGRATIONS_EVENT_INTEGRATION_DESCRIPTION

**Resource Types:** AWS::AppIntegrations::EventIntegration

**Trigger type:** Configuration changes

**AWS Region:** Only available in Africa (Cape Town), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appintegrations-event-integration-tagged

Checks if Amazon AppIntegrations event integrations have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPINTEGRATIONS_EVENT_INTEGRATION_TAGGED

**Resource Types:** AWS::AppIntegrations::EventIntegration

**Trigger type:** Configuration changes

**AWS Region:** Only available in Africa (Cape Town), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-gateway-route-tagged

Checks if AWS App Mesh gateway routes have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPMESH_GATEWAY_ROUTE_TAGGED

**Resource Types:** AWS::AppMesh::GatewayRoute

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-mesh-deny-tcp-forwarding

Checks if proxies for AWS App Mesh service meshes do not forward TCP traffic directly to services that aren't deployed with a proxy that is defined in the mesh. The rule is NON_COMPLIANT if configuration.Spec.EgressFilter.Type is set to 'ALLOW_ALL'.

**Identifier:** APPMESH_MESH_DENY_TCP_FORWARDING

**Resource Types:** AWS::AppMesh::Mesh

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-mesh-tagged

Checks if AWS App Mesh meshes have tags. Optionally, you can specify tag keys for the rule to check. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPMESH_MESH_TAGGED

**Resource Types:** AWS::AppMesh::Mesh

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-route-tagged

Checks if AWS App Mesh routes have tags. Optionally, you can specify tag keys for the rule to check. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPMESH_ROUTE_TAGGED

**Resource Types:** AWS::AppMesh::Route

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-gateway-backend-defaults-tls

Checks if backend defaults for AWS App Mesh virtual gateways require the virtual gateways to communicate with all ports using TLS. The rule is NON_COMPLIANT if configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce is false.

**Identifier:** APPMESH_VIRTUAL_GATEWAY_BACKEND_DEFAULTS_TLS

**Resource Types:** AWS::AppMesh::VirtualGateway

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-gateway-logging-file-path-exists

Checks if AWS App Mesh virtual gateways have a file path to write access logs to. The rule is NON_COMPLIANT if configuration.Spec.Logging.AccessLog.File.Path does not exist.

**Identifier:** APPMESH_VIRTUAL_GATEWAY_LOGGING_FILE_PATH_EXISTS

**Resource Types:** AWS::AppMesh::VirtualGateway

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-gateway-tagged

Checks if AWS App Mesh virtual gateways have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPMESH_VIRTUAL_GATEWAY_TAGGED

**Resource Types:** AWS::AppMesh::VirtualGateway

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-node-backend-defaults-tls-on

Checks if backend defaults for AWS App Mesh virtual nodes require the virtual nodes to communicate with all ports using TLS. The rule is NON_COMPLIANT if configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce is false.

**Identifier:** APPMESH_VIRTUAL_NODE_BACKEND_DEFAULTS_TLS_ON

**Resource Types:** AWS::AppMesh::VirtualNode

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-node-cloud-map-ip-pref-check

Checks if an AWS App Mesh virtual node is configured with the specified IP preference for AWS Cloud Map service discovery. The rule is NON_COMPLIANT if the virtual node is not configured with the IP preference specified in the required rule parameter.

**Identifier:** APPMESH_VIRTUAL_NODE_CLOUD_MAP_IP_PREF_CHECK

**Resource Types:** AWS::AppMesh::VirtualNode

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

ipPreference, Type: String

The IP preference value for AWS Cloud Map service discovery. The rule is NON_COMPLIANT if a virtual node is configured with a value that does not match this value. Valid values include: 'IPv6_PREFERRED', 'IPv4_PREFERRED', 'IPv4_ONLY', and 'IPv6_ONLY'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-node-dns-ip-pref-check

Checks if an AWS App Mesh virtual node is configured with the specified IP preference for DNS service discovery. The rule is NON_COMPLIANT if the virtual node is not configured with the IP preference specified in the required rule parameter.

**Identifier:** APPMESH_VIRTUAL_NODE_DNS_IP_PREF_CHECK

**Resource Types:** AWS::AppMesh::VirtualNode

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

ipPreference, Type: String

The IP preference value for DNS service discovery. The rule is NON_COMPLIANT if a virtual node is configured with a value that does not match this value. Valid values include: 'IPv6_PREFERRED', 'IPv4_PREFERRED', 'IPv4_ONLY', and 'IPv6_ONLY'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-node-logging-file-path-exists

Checks if AWS App Mesh virtual nodes have a file path to write access logs to. The rule is NON_COMPLIANT if configuration.Spec.Logging.AccessLog.File.Path does not exist.

**Identifier:** APPMESH_VIRTUAL_NODE_LOGGING_FILE_PATH_EXISTS

**Resource Types:** AWS::AppMesh::VirtualNode

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-node-tagged

Checks if AWS App Mesh virtual nodes have tags. Optionally, you can specify tag keys for the rule to check. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPMESH_VIRTUAL_NODE_TAGGED

**Resource Types:** AWS::AppMesh::VirtualNode

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud

(US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-router-tagged

Checks if AWS App Mesh virtual routers have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPMESH_VIRTUAL_ROUTER_TAGGED

**Resource Types:** AWS::AppMesh::VirtualRouter

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appmesh-virtual-service-tagged

Checks if AWS App Mesh virtual services have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPMESH_VIRTUAL_SERVICE_TAGGED

**Resource Types:** AWS::AppMesh::VirtualService

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## approved-amis-by-id

Checks if EC2 instances are using specified Amazon Machine Images (AMIs). Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are NON_COMPLIANT.

**Identifier:** APPROVED_AMIS_BY_ID

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

amiIds, Type: CSV

Comma-separated list of up to 21 AMI IDs. There is a 1024 characters limit.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## approved-amis-by-tag

Checks if EC2 instances are using specified Amazon Machine Images (AMIs). Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags are NON_COMPLIANT.

**Identifier:** APPROVED_AMIS_BY_TAG

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

amisByTagKeyAndValue, Type: StringMap, Default: tag-key:tag-value,other-tag-key

Comma-separated list of up to 10 AMIs tags (tag-key:tag-value). For example, tag-key1 matches AMIs with tag-key1; tag-key2:value2 matches tag-key2 with the value 2.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apprunner-service-in-vpc

Checks if AWS App Runner services route egress traffic through custom VPC. The rule is NON_COMPLIANT if configuration.NetworkConfiguration.EgressConfiguration.EgressType is equal to DEFAULT.

**Identifier:** APPRUNNER_SERVICE_IN_VPC

**Resource Types:** AWS::AppRunner::Service

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apprunner-service-ip-address-type-check

Checks if an AWS App Runner service is configured with the specified IP address type for incoming public network configuration. The rule is NON_COMPLIANT if the service is not configured with the IP address type specified in the required rule parameter.

**Identifier:** APPRUNNER_SERVICE_IP_ADDRESS_TYPE_CHECK

**Resource Types:** AWS::AppRunner::Service

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

ipAddressType, Type: String

The IP address type value for the rule to check. The rule is NON_COMPLIANT if an AWS App Runner service is configured with a value that does not match this value. Valid values include: 'IPV4', 'DUAL_STACK'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apprunner-service-max-unhealthy-threshold

Checks if an AWS App Runner service is configured to have an unhealthy threshold less than or equal to the specified value. The rule is NON_COMPLIANT if the unhealthy threshold is greater than the value specified in the required rule parameter.

**Identifier:** APPRUNNER_SERVICE_MAX_UNHEALTHY_THRESHOLD

**Resource Types:** AWS::AppRunner::Service

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

maxUnhealthyThreshold, Type: int

The maximum unhealthy threshold value for the rule to check. The rule is NON_COMPLIANT if an AWS App Runner service is configured with an unhealthy threshold greater than this value. Valid values are 1 to 20

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apprunner-service-no-public-access

Checks if AWS AppRunner Services are not publicly accessible. The rule is NON_COMPLIANT if service.configuration.NetworkConfiguration.IngressConfiguration.IsPubliclyAccessible is False.

**Identifier:** APPRUNNER_SERVICE_NO_PUBLIC_ACCESS

**Resource Types:** AWS::AppRunner::Service

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apprunner-service-observability-enabled

Checks if AWS App Runner services have observability enabled. The rule is NON_COMPLIANT if configuration.ObservabilityConfiguration.ObservabilityEnabled is false'.

**Identifier:** APPRUNNER_SERVICE_OBSERVABILITY_ENABLED

**Resource Types:** AWS::AppRunner::Service

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apprunner-service-tagged

Checks if AWS App Runner services have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPRUNNER_SERVICE_TAGGED

**Resource Types:** AWS::AppRunner::Service

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## apprunner-vpc-connector-tagged

Checks if AWS App Runner VPC connectors have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APPRUNNER_VPC_CONNECTOR_TAGGED

**Resource Types:** AWS::AppRunner::VpcConnector

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appstream-fleet-in-vpc

Checks if Amazon AppStream 2.0 fleets use an Amazon Virtual Private Cloud (Amazon VPC). The rule is NON_COMPLIANT if configuration.VpcConfig does not exist. The rule does not check Elastic fleets.

**Identifier:** APPSTREAM_FLEET_IN_VPC

**Resource Types:** AWS::AppStream::Fleet

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appsync-associated-with-waf

Checks if AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL.

**Identifier:** APPSYNC_ASSOCIATED_WITH_WAF

**Resource Types:** AWS::AppSync::GraphQLApi

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

wafWebAclARNs (Optional), Type: CSV

Comma-separated list of Amazon Resource Names (ARNs) for authorized web ACLs.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appsync-authorization-check

Checks if an AWS AppSync API is using allowed authorization mechanisms. The rule is NON_COMPLIANT if an unapproved authorization mechanism is being used.

**Identifier:** APPSYNC_AUTHORIZATION_CHECK

**Resource Types:** AWS::AppSync::GraphQLApi

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

AllowedAuthorizationTypes, Type: CSV

> Comma-separated list of allowed AWS AppSync authorization mechanisms. Allowed values are: 'API_KEY', 'AWS_LAMBDA', 'AWS_IAM', 'OPENID_CONNECT', 'AMAZON_COGNITO_USER_POOLS'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appsync-cache-ct-encryption-at-rest

Checks if an AWS AppSync API cache has encryption at rest enabled. This rule is NON_COMPLIANT if 'AtRestEncryptionEnabled' is false.

**Identifier:** APPSYNC_CACHE_CT_ENCRYPTION_AT_REST

**Resource Types:** AWS::AppSync::ApiCache

**Trigger type:** Configuration changes

**AWS Region:** Only available in Middle East (Bahrain), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appsync-cache-ct-encryption-in-transit

Checks if an AWS AppSync API cache has encryption in transit enabled. The rule is NON_COMPLIANT if 'TransitEncryptionEnabled' is false.

**Identifier:** APPSYNC_CACHE_CT_ENCRYPTION_IN_TRANSIT

**Resource Types:** AWS::AppSync::ApiCache

**Trigger type:** Configuration changes

**AWS Region:** Only available in Middle East (Bahrain), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appsync-cache-encryption-at-rest

Checks if an AWS AppSync API cache has encryption at rest enabled. This rule is NON_COMPLIANT if 'AtRestEncryptionEnabled' is false.

**Identifier:** APPSYNC_CACHE_ENCRYPTION_AT_REST

**Resource Types:** AWS::AppSync::GraphQLApi

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appsync-graphql-api-xray-enabled

Checks if AWS AppSync GraphQL APIs have AWS X-Ray tracing enabled. The rule is NON_COMPLIANT if configuration.XrayEnabled is false.

**Identifier:** APPSYNC_GRAPHQL_API_XRAY_ENABLED

**Resource Types:** AWS::AppSync::GraphQLApi

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## appsync-logging-enabled

Checks if an AWS AppSync API has field level logging enabled. The rule is NON_COMPLIANT if field level logging is not enabled, or if the field logging levels for the AppSync API do not match the values specified in the '`fieldLoggingLevel`' parameter.

**Identifier:** APPSYNC_LOGGING_ENABLED

**Resource Types:** AWS::AppSync::GraphQLApi

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

fieldLoggingLevel (Optional), Type: CSV

Comma-separated list of field logging levels for the rule to check. For example, "ERROR, INFO".

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## aps-rule-groups-namespace-tagged

Checks if Amazon Managed Service for Prometheus rule groups namepaces have tags. You can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** APS_RULE_GROUPS_NAMESPACE_TAGGED

**Resource Types:** AWS::APS::RuleGroupsNamespace

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia

Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## athena-data-catalog-description

Checks if Amazon Athena data catalogs have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** ATHENA_DATA_CATALOG_DESCRIPTION

**Resource Types:** AWS::Athena::DataCatalog

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## athena-prepared-statement-description

Checks if Amazon Athena prepared statements have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** ATHENA_PREPARED_STATEMENT_DESCRIPTION

**Resource Types:** AWS::Athena::PreparedStatement

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## athena-workgroup-description

Checks if Amazon Athena workgroups have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** ATHENA_WORKGROUP_DESCRIPTION

**Resource Types:** AWS::Athena::WorkGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## athena-workgroup-encrypted-at-rest

Checks if an Amazon Athena workgroup is encrypted at rest. The rule is NON_COMPLIANT if encryption of data at rest is not enabled for an Athena workgroup.

**Identifier:** ATHENA_WORKGROUP_ENCRYPTED_AT_REST

**Resource Types:** AWS::Athena::WorkGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## athena-workgroup-enforce-workgroup-configuration

Checks if Amazon Athena workgroups using Athena engine enforce workgroup configuration to override client-side settings. The rule is NON_COMPLIANT if configuration.WorkGroupConfiguration.EnforceWorkGroupConfiguration is false.

**Identifier:** ATHENA_WORKGROUP_ENFORCE_WORKGROUP_CONFIGURATION

**Resource Types:** AWS::Athena::WorkGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## athena-workgroup-engine-version-auto-upgrade

Checks if Amazon Athena workgroups using Athena engine are configured to auto upgrade. The rule is NON_COMPLIANT if configuration.WorkGroupConfiguration.EngineVersion.SelectedEngineVersion is not 'AUTO'.

**Identifier:** ATHENA_WORKGROUP_ENGINE_VERSION_AUTO_UPGRADE

**Resource Types:** AWS::Athena::WorkGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## athena-workgroup-logging-enabled

Checks if Amazon Athena WorkGroup publishes usage metrics to Amazon CloudWatch. The rule is NON_COMPLIANT if an Amazon Athena WorkGroup 'PublishCloudWatchMetricsEnabled' is set to false.

**Identifier:** ATHENA_WORKGROUP_LOGGING_ENABLED

**Resource Types:** AWS::Athena::WorkGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## auditmanager-assessment-tagged

Checks if AWS Audit Manager assessments have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** AUDITMANAGER_ASSESSMENT_TAGGED

**Resource Types:** AWS::AuditManager::Assessment

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### aurora-global-database-encryption-at-rest

Checks if Amazon Aurora Global Databases have storage encryption enabled. This rule is NON_COMPLIANT if an Amazon Aurora Global Database does not have storage encryption enabled.

**Identifier:** AURORA_GLOBAL_DATABASE_ENCRYPTION_AT_REST

**Resource Types:** AWS::RDS::GlobalCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### aurora-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon Aurora DB clusters. The rule is NON_COMPLIANT if the Amazon Relational Database Service (Amazon RDS) DB Cluster does not have a corresponding recovery point created within the specified time period.

**Identifier:** AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Aurora DB clusters for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Aurora DB cluster for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## aurora-meets-restore-time-target

Checks if the restore time of Amazon Aurora DB clusters meets the specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of an Aurora DB Cluster is greater than maxRestoreTime minutes.

**Identifier:** AURORA_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags of Aurora DB clusters for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Aurora DB cluster for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## aurora-mysql-backtracking-enabled

Checks if an Amazon Aurora MySQL cluster has backtracking enabled. The rule is NON_COMPLIANT if the Aurora cluster uses MySQL and it does not have backtracking enabled.

**Identifier:** AURORA_MYSQL_BACKTRACKING_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Osaka), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

BacktrackWindowInHours (Optional), Type: double

Amount of time in hours (up to 72) to backtrack your Aurora MySQL cluster.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## aurora-mysql-cluster-audit-logging

Checks if Amazon Aurora MySQL DB clusters have audit logging enabled. The rule is NON_COMPLIANT if a DB cluster does not have audit logging enabled.

**Identifier:** AURORA_MYSQL_CLUSTER_AUDIT_LOGGING

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## aurora-resources-in-logically-air-gapped-vault

Checks if Amazon Aurora DB clusters are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon Aurora DB cluster is not in a logically air-gapped vault within the specified time period.

**Identifier:** AURORA_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Aurora DB clusters for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Aurora DB cluster for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 2184 for hours, 91 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## aurora-resources-protected-by-backup-plan

Checks if Amazon Aurora DB clusters are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon Relational Database Service (Amazon RDS) Database Cluster is not protected by a backup plan.

**Identifier:** AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Aurora DB clusters for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Aurora DB cluster for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## autoscaling-capacity-rebalancing

Checks if Capacity Rebalancing is enabled for Amazon EC2 Auto Scaling groups that use multiple instance types. The rule is NON_COMPLIANT if capacity Rebalancing is not enabled.

**Identifier:** AUTOSCALING_CAPACITY_REBALANCING

**Resource Types:** AWS::AutoScaling::AutoScalingGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## autoscaling-group-elb-healthcheck-required

Checks if your Amazon EC2 Auto Scaling groups that are associated with an Elastic Load Balancer use Elastic Load Balancing health checks. The rule is NON_COMPLIANT if the Amazon EC2 Auto Scaling groups are not using Elastic Load Balancing health checks.

**Identifier:** AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

**Resource Types:** AWS::AutoScaling::AutoScalingGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*The valid values are EC2 (default), ELB, and VPC_LATTICE. The VPC_LATTICE health check type is reserved for use with VPC Lattice, which is in preview release and is subject to change. For more information, see Health checks for Auto Scaling instances in the Amazon EC2 Auto Scaling User Guide.

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## autoscaling-launchconfig-requires-imdsv2

Checks whether only IMDSv2 is enabled. This rule is NON_COMPLIANT if the Metadata version is not included in the launch configuration or if both Metadata V1 and V2 are enabled.

**Identifier:** AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

**Resource Types:** AWS::AutoScaling::LaunchConfiguration

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## autoscaling-launch-config-hop-limit

Checks the number of network hops that the metadata token can travel. This rule is NON_COMPLIANT if the Metadata response hop limit is greater than 1.

**Identifier:** AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

**Resource Types:** AWS::AutoScaling::LaunchConfiguration

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## autoscaling-launch-config-public-ip-disabled

Checks if Amazon EC2 Auto Scaling groups have public IP addresses enabled through Launch Configurations. The rule is NON_COMPLIANT if the Launch Configuration for an Amazon EC2 Auto Scaling group has AssociatePublicIpAddress set to 'true'.

**Identifier:** AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

**Resource Types:** AWS::AutoScaling::LaunchConfiguration

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### autoscaling-launch-template

Checks if an Amazon Elastic Compute Cloud (EC2) Auto Scaling group is created from an EC2 launch template. The rule is NON_COMPLIANT if the scaling group is not created from an EC2 launch template.

**Identifier:** AUTOSCALING_LAUNCH_TEMPLATE

**Resource Types:** AWS::AutoScaling::AutoScalingGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## autoscaling-multiple-az

Checks if the Auto Scaling group spans multiple Availability Zones. The rule is NON_COMPLIANT if the Auto Scaling group does not span multiple Availability Zones.

**Identifier:** AUTOSCALING_MULTIPLE_AZ

**Resource Types:** AWS::AutoScaling::AutoScalingGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

minAvailabilityZones (Optional), Type: int

Minimum number of expected Availability zones.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## autoscaling-multiple-instance-types

Checks if an Amazon EC2 Auto Scaling group uses multiple instance types. The rule is NON_COMPLIANT if the Amazon EC2 Auto Scaling group has only one instance type defined. This rule does not evaluate attribute-based instance types.

**Identifier:** AUTOSCALING_MULTIPLE_INSTANCE_TYPES

**Resource Types:** AWS::AutoScaling::AutoScalingGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## backup-plan-min-frequency-and-min-retention-check

Checks if a backup plan has a backup rule that satisfies the required frequency and retention period. The rule is NON_COMPLIANT if recovery points are not created at least as often as the specified frequency or expire before the specified period.

**Identifier:** BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

**Resource Types:** AWS::Backup::BackupPlan

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredFrequencyValue (Optional), Type: int, Default: 1

Numerical value for required backup frequency. Maximum of 24 for hours, 31 for days.

requiredRetentionDays (Optional), Type: int, Default: 35

Required retention period in days.

requiredFrequencyUnit (Optional), Type: String, Default: days

Unit of time for required backup frequency. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## backup-recovery-point-encrypted

Checks if a recovery point is encrypted. The rule is NON_COMPLIANT if the recovery point is not encrypted.

**Identifier:** BACKUP_RECOVERY_POINT_ENCRYPTED

**Resource Types:** AWS::Backup::RecoveryPoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## backup-recovery-point-manual-deletion-disabled

Checks if a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions).

> **Note**
>
> **Wildcard required for `"Resource"` and `"Principal"` of the Deny statement**
> The rule requires that the `"Resource"` and `"Principal"` of the Deny statement must have a wildcard in the vault access policy. Otherwise, the rule returns NON_COMPLIANT.

**Identifier:** BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

**Resource Types:** AWS::Backup::BackupVault

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

principalArnList (Optional), Type: CSV

Comma-separated list of AWS Identity and Access Management (IAM) Amazon Resource Names (ARNs) for the rule to NOT check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## backup-recovery-point-minimum-retention-check

Checks if a recovery point expires no earlier than after the specified period. The rule is NON_COMPLIANT if the recovery point has a retention point that is less than the required retention period.

**Identifier:** BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

**Resource Types:** AWS::Backup::RecoveryPoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredRetentionDays (Optional), Type: int, Default: 35

Required retention period in days.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-compute-environment-enabled

Checks if AWS Batch compute environments are enabled. The rule is NON_COMPLIANT if configuration.State is 'DISABLED'.

**Identifier:** BATCH_COMPUTE_ENVIRONMENT_ENABLED

**Resource Types:** AWS::Batch::ComputeEnvironment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-compute-environment-managed

Checks if AWS Batch compute environments are managed. The rule is NON_COMPLIANT if configuration.Type is 'UNMANAGED'.

**Identifier:** BATCH_COMPUTE_ENVIRONMENT_MANAGED

**Resource Types:** AWS::Batch::ComputeEnvironment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-compute-environment-tagged

Checks if AWS Batch compute environments have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** BATCH_COMPUTE_ENVIRONMENT_TAGGED

**Resource Types:** AWS::Batch::ComputeEnvironment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-job-queue-enabled

Checks if AWS Batch job queues are enabled. The rule is NON_COMPLIANT if configuration.State is 'DISABLED'.

**Identifier:** BATCH_JOB_QUEUE_ENABLED

**Resource Types:** AWS::Batch::JobQueue

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-job-queue-tagged

Checks if AWS Batch job queues have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** BATCH_JOB_QUEUE_TAGGED

**Resource Types:** AWS::Batch::JobQueue

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### batch-managed-compute-environment-using-launch-template

Checks if AWS Batch managed compute environments are configured using a launch template. The rule is NON_COMPLIANT if configuration.ComputeResources.LaunchTemplate does not exist.

**Identifier:** BATCH_MANAGED_COMPUTE_ENVIRONMENT_USING_LAUNCH_TEMPLATE

**Resource Types:** AWS::Batch::ComputeEnvironment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### batch-managed-compute-env-allocation-strategy-check

Checks if an AWS Batch managed compute environment is configured with a specified allocation strategy. The rule is NON_COMPLIANT if the compute environment is not configured with an allocation strategy specified in the required rule parameter.

**Identifier:** BATCH_MANAGED_COMPUTE_ENV_ALLOCATION_STRATEGY_CHECK

**Resource Types:** AWS::Batch::ComputeEnvironment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

allocationStrategy, Type: CSV

> Comma-separated list of allocation strategies for the rule to check. Valid values include: 'BEST_FIT', 'BEST_FIT_PROGRESSIVE', 'SPOT_CAPACITY_OPTIMIZED', and 'SPOT_PRICE_CAPACITY_OPTIMIZED'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-managed-compute-env-compute-resources-tagged

Checks if AWS Batch managed compute environments compute resources have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. Tags starting with 'aws:' are not checked.

**Identifier:** BATCH_MANAGED_COMPUTE_ENV_COMPUTE_RESOURCES_TAGGED

**Resource Types:** AWS::Batch::ComputeEnvironment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-managed-spot-compute-environment-max-bid

Checks if an AWS Batch managed Spot compute environment is configured to have a bid percentage less than or equal to the specified value. The rule is NON_COMPLIANT if the bid percentage is greater than the value specified in the required rule parameter.

**Identifier:** BATCH_MANAGED_SPOT_COMPUTE_ENVIRONMENT_MAX_BID

**Resource Types:** AWS::Batch::ComputeEnvironment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxBidPercentage, Type: int

The maximum bid percentage value for the rule to check. The rule is NON_COMPLIANT if an AWS Batch managed Spot compute environment is configured with a bid percentage greater than this value. Valid values are 1 to 100.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## batch-scheduling-policy-tagged

Checks if AWS Batch scheduling policies have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** BATCH_SCHEDULING_POLICY_TAGGED

**Resource Types:** AWS::Batch::SchedulingPolicy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## beanstalk-enhanced-health-reporting-enabled

Checks if an AWS Elastic Beanstalk environment is configured for enhanced health reporting. The rule is COMPLIANT if the environment is configured for enhanced health reporting. The rule is NON_COMPLIANT if the environment is configured for basic health reporting.

**Identifier:** BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

**Resource Types:** AWS::ElasticBeanstalk::Environment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cassandra-keyspace-tagged

Checks if Amazon Keyspaces (for Apache Cassandra) keyspaces have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** CASSANDRA_KEYSPACE_TAGGED

**Resource Types:** AWS::Cassandra::Keyspace

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Middle East (Bahrain), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), Asia Pacific (Hong Kong), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## clb-desync-mode-check

Checks if Classic Load Balancers (CLB) are configured with a user defined Desync mitigation mode. The rule is NON_COMPLIANT if CLB Desync mitigation mode does not match with user defined Desync mitigation mode.

**Identifier:** CLB_DESYNC_MODE_CHECK

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

desyncMode, Type: CSV

> Comma-separated list of values. You can select a max of two. Valid values include 'Defensive', 'Strictest', and 'Monitor'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## clb-multiple-az

Checks if a Classic Load Balancer spans multiple Availability Zones (AZs). The rule is NON_COMPLIANT if a Classic Load Balancer spans less than 2 AZs or does not span number of AZs mentioned in the `minAvailabilityZones` parameter (if provided).

**Identifier:** CLB_MULTIPLE_AZ

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

minAvailabilityZones (Optional), Type: int

Desired minimum number of expected AZs. Valid values are between 2 and 10, both inclusive. Default value is 2 if parameter is not specified.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudformation-stack-drift-detection-check

Checks if the actual configuration of a AWS CloudFormation (CloudFormation) stack differs, or has drifted, from the expected configuration. A stack is considered to have drifted if one or more of its resources differ from their expected configuration. The rule and the stack are COMPLIANT when the stack drift status is IN_SYNC. The rule is NON_COMPLIANT if the stack drift status is DRIFTED.

> **Note**
>
> This rule performs the DetectStackDrift operation on each stack in your account. The DetectStackDrift operation can take up to several minutes, depending on the number of resources contained within the stack. Given that the maximum execution time of this rule is limited to 15 mins, it is possible that the rule times out before it completes the evaluation of all the stacks in your account.
> If you encounter this issue, it is suggested that you to restrict the number of stacks in-scope for the rule, using tags. You can do the following:
>
> 1. Divide your stacks into groups, each with a different tag.
> 2. Apply the same tag to all the stacks in that group.

3. Have multiple instances of this rule in your account, each scoped by a different tag. This allows each instance of the rule to only process the stacks which have the corresponding tag mentioned in its scope.

**Identifier:** CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

**Resource Types:** AWS::CloudFormation::Stack

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Melbourne), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

cloudformationRoleArn, Type: String

The Amazon Resource Name (ARN) of the IAM role with policy permissions to detect drift for CloudFormation stacks. For information on required IAM permissions for the role, see Detecting unmanaged configuration changes to stacks and resources | Considerations when detecting drift in the *CloudFormation User Guide*.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudformation-stack-notification-check

Checks if your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally checks if specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications.

**Identifier:** CLOUDFORMATION_STACK_NOTIFICATION_CHECK

**Resource Types:** AWS::CloudFormation::Stack

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

snsTopic2 (Optional), Type: String

SNS topic ARN.

snsTopic1 (Optional), Type: String

SNS topic ARN.

snsTopic5 (Optional), Type: String

SNS topic ARN.

snsTopic4 (Optional), Type: String

SNS topic ARN.

snsTopic3 (Optional), Type: String

SNS topic ARN.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudformation-stack-service-role-check

Checks if AWS CloudFormation stacks are using service roles. The rule is NON_COMPLIANT if a CloudFormation stack does not have service role associated with it.

**Identifier:** CLOUDFORMATION_STACK_SERVICE_ROLE_CHECK

**Resource Types:** AWS::CloudFormation::Stack

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudformation-termination-protection-check

Checks if an AWS CloudFormation stack has termination protection enabled. This rule is NON_COMPLIANT if termination protection is not enabled on a CloudFormation stack.

**Identifier:** CLOUDFORMATION_TERMINATION_PROTECTION_CHECK

**Resource Types:** AWS::CloudFormation::Stack

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-accesslogs-enabled

Checks if Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket using standard logging (legacy). The rule is NON_COMPLIANT if a CloudFront distribution does not have legacy logging configured.

**Identifier:** CLOUDFRONT_ACCESSLOGS_ENABLED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

S3BucketName (Optional), Type: String

The name of the Amazon S3 bucket for storing server access logs

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-associated-with-waf

Checks if Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL.

**Identifier:** CLOUDFRONT_ASSOCIATED_WITH_WAF

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

wafWebAclIds (Optional), Type: CSV

Comma-separated list of web ACL IDs for WAF or web ACL Amazon Resource Names (ARNs) for WAFV2

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-custom-ssl-certificate

Checks if the certificate associated with an Amazon CloudFront distribution is the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate.

**Identifier:** CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-default-root-object-configured

Checks if an Amazon CloudFront distribution is configured to return a specific object that is the default root object. The rule is NON_COMPLIANT if Amazon CloudFront distribution does not have a default root object configured.

**Identifier:** CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-distribution-key-group-enabled

Checks if Amazon CloudFront distributions are configured to use only trusted key groups for signed URL or signed cookie authentication for all cache behaviors. The rule is NON_COMPLIANT if any cache behavior in the distribution is using trusted signers.

**Identifier:** CLOUDFRONT_DISTRIBUTION_KEY_GROUP_ENABLED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-no-deprecated-ssl-protocols

Checks if CloudFront distributions are using deprecated SSL protocols for HTTPS communication between CloudFront edge locations and custom origins. This rule is NON_COMPLIANT for a CloudFront distribution if any 'OriginSslProtocols' includes 'SSLv3'.

**Identifier:** CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-origin-access-identity-enabled

Checks if CloudFront distribution with Amazon S3 Origin type has origin access identity configured. The rule is NON_COMPLIANT if the CloudFront distribution is backed by S3 and any origin type is not OAI configured, or the origin is not an S3 bucket.

> **Note**
>
> The rule does not return `NOT_APPLICABLE` if the origin is not an S3 bucket.

**Identifier:** CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-origin-failover-enabled

Checks if an origin group is configured for the distribution of at least two origins in the origin group for Amazon CloudFront. The rule is NON_COMPLIANT if there are no origin groups for the distribution.

**Identifier:** CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-origin-lambda-url-oac-enabled

Checks if Amazon CloudFront distributions with Amazon Lambda Function URL origins have origin access control (OAC) enabled. The rule is NON_COMPLIANT if any Lambda Function URL origin in a CloudFront distribution does not have OAC enabled.

**Identifier:** CLOUDFRONT_ORIGIN_LAMBDA_URL_OAC_ENABLED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-s3-origin-access-control-enabled

Checks if an Amazon CloudFront distribution with an Amazon Simple Storage Service (Amazon S3) Origin type has origin access control (OAC) enabled. The rule is NON_COMPLIANT for CloudFront distributions with Amazon S3 origins that don't have OAC enabled.

**Identifier:** CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-s3-origin-non-existent-bucket

Checks if Amazon CloudFront distributions point to a non-existent S3 bucket. The rule is NON_COMPLIANT if `S3OriginConfig` for a CloudFront distribution points to a non-existent S3 bucket. The rule does not evaluate S3 buckets with static website hosting.

**Identifier:** CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Periodic

**AWS Region:** Only available in China (Beijing), US East (N. Virginia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-security-policy-check

Checks if Amazon CloudFront distributions are using a minimum security policy and cipher suite of TLSv1.2 or greater for viewer connections. This rule is NON_COMPLIANT for a CloudFront distribution if the minimumProtocolVersion is below TLSv1.2_2018.

**Identifier:** CLOUDFRONT_SECURITY_POLICY_CHECK

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-sni-enabled

Checks if Amazon CloudFront distributions are using a custom SSL certificate and are configured to use SNI to serve HTTPS requests. The rule is NON_COMPLIANT if a custom SSL certificate is associated but the SSL support method is a dedicated IP address.

**Identifier:** CLOUDFRONT_SNI_ENABLED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-ssl-policy-check

Checks if Amazon CloudFront distributions are configured with the specified security policies.The rule is NON_COMPLIANT if a CloudFront Distribution is not configured with security policies that you specify.

**Identifier:** CLOUDFRONT_SSL_POLICY_CHECK

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

securityPolicies, Type: CSV

Comma-separated list of CloudFront distribution security policies for the rule to check. For example: "TLSv1.2_2018, TLSv1.2_2019, TLSv1.2_2021". For a list of valid value, see the Amazon CloudFront Developer Guide.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-traffic-to-origin-encrypted

Checks if Amazon CloudFront distributions are encrypting traffic to custom origins. The rule is NON_COMPLIANT if ‘OriginProtocolPolicy’ is ‘http-only’ or if ‘OriginProtocolPolicy’ is ‘match-viewer’ and ‘ViewerProtocolPolicy’ is ‘allow-all’.

**Identifier:** CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudfront-viewer-policy-https

Checks whether your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the defaultCacheBehavior or for the CacheBehaviors.

**Identifier:** CLOUDFRONT_VIEWER_POLICY_HTTPS

**Resource Types:** AWS::CloudFront::Distribution

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudtrail-all-read-s3-data-event-check

Checks if an AWS CloudTrail multi-Region trail is enabled and logs all read S3 data events for your buckets. The rule is NON_COMPLIANT if no multi-Region trail logs all read S3 data event types for all current and future S3 buckets.

**Identifier:** CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudtrail-all-write-s3-data-event-check

Checks if an AWS CloudTrail multi-Region trail is enabled and logs all write S3 data events for your buckets. The rule is NON_COMPLIANT if no multi-Region trail logs all write S3 data event types for all current and future S3 buckets.

**Identifier:** CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudtrail-s3-bucket-access-logging

Checks if the S3 bucket configurations for your AWS CloudTrail logs have Amazon S3 server access logging enabled. The rule is NON_COMPLIANT if at least one S3 bucket for a CloudTrail trail does not have S3 server access logging enabled.

**Identifier:** CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

**Resource Types:** AWS::CloudTrail::Trail

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudtrail-s3-bucket-public-access-prohibited

Checks if the S3 bucket configurations for your AWS CloudTrail logs block public access. The rule is NON_COMPLIANT if at least one S3 bucket for a CloudTrail trail is publicly accessible.

**Identifier:** CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBITED

**Resource Types:** AWS::CloudTrail::Trail

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudtrail-s3-dataevents-enabled

Checks if at least one AWS CloudTrail trail is logging Amazon Simple Storage Service (Amazon S3) data events for all S3 buckets. The rule is NON_COMPLIANT if there are trails or if no trails record S3 data events.

**Identifier:** CLOUDTRAIL_S3_DATAEVENTS_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

S3BucketNames (Optional), Type: String

Comma-separated list of S3 bucket names for which data events logging should be enabled. Default behavior checks for all S3 buckets.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudtrail-security-trail-enabled

Checks that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following:

- records global service events
- is a multi-region trail
- has Log file validation enabled
- encrypted with a KMS key
- records events for reads and writes
- records management events
- does not exclude any management events

This rule is NON_COMPLIANT if no trails meet all of the criteria mentioned above.

**Identifier:** CLOUDTRAIL_SECURITY_TRAIL_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudwatch-alarm-action-check

Checks if CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally checks if any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter.

**Identifier:** CLOUDWATCH_ALARM_ACTION_CHECK

**Resource Types:** AWS::CloudWatch::Alarm

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

okActionRequired, Type: String, Default: false

Alarms have at least one action when the alarm transitions to an OK state from any other state.

insufficientDataActionRequired, Type: String, Default: true

Alarms have at least one action when the alarm transitions to the INSUFFICIENT_DATA state from any other state.

alarmActionRequired, Type: String, Default: true

Alarms have at least one action.

action1 (Optional), Type: String

The action to execute, specified as an ARN.

action2 (Optional), Type: String

The action to execute, specified as an ARN.

action3 (Optional), Type: String

The action to execute, specified as an ARN.

action4 (Optional), Type: String

The action to execute, specified as an ARN.

action5 (Optional), Type: String

The action to execute, specified as an ARN.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### cloudwatch-alarm-action-enabled-check

Checks if Amazon CloudWatch alarms actions are in enabled state. The rule is NON_COMPLIANT if the CloudWatch alarms actions are not in enabled state.

**Identifier:** CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

**Resource Types:** AWS::CloudWatch::Alarm

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### cloudwatch-alarm-resource-check

Checks if a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm.

**Identifier:** CLOUDWATCH_ALARM_RESOURCE_CHECK

**Resource Types:** AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

resourceType, Type: String

AWS resource type. The value can be one of the following: AWS::EC2::Volume, AWS::EC2::Instance, AWS::RDS::DBCluster, or AWS::S3::Bucket.

metricName, Type: String

The name for the metric associated with the alarm (for example, 'CPUUtilization' for EC2 instances).

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudwatch-alarm-settings-check

Checks whether CloudWatch alarms with the given metric name have the specified settings.

**Identifier:** CLOUDWATCH_ALARM_SETTINGS_CHECK

**Resource Types:** AWS::CloudWatch::Alarm

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

metricName, Type: String

The name for the metric associated with the alarm.

period (Optional), Type: int, Default: 300

The period, in seconds, during which the specified statistic is applied.

statistic (Optional), Type: String

The statistic for the metric associated with the alarm (for example, 'Average' or 'Sum').

comparisonOperator (Optional), Type: String

The operation for comparing the specified statistic and threshold (for example, 'GreaterThanThreshold').

threshold (Optional), Type: int

The value against which the specified statistic is compared.

evaluationPeriods (Optional), Type: int

The number of periods over which data is compared to the specified threshold.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudwatch-log-group-encrypted

Checks if Amazon CloudWatch Log Groups are encrypted with any AWS KMS key or a specified AWS KMS key Id. The rule is NON_COMPLIANT if a CloudWatch Log Group is not encrypted with a KMS key or is encrypted with a KMS key not supplied in the rule parameter.

**Identifier:** CLOUDWATCH_LOG_GROUP_ENCRYPTED

**Resource Types:** AWS::Logs::LogGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

KmsKeyId (Optional), Type: String

Amazon Resource Name (ARN) of the ID for the KMS key that is used to encrypt the log group.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloudwatch-metric-stream-tagged

Checks if Amazon CloudWatch metric streams have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** CLOUDWATCH_METRIC_STREAM_TAGGED

**Resource Types:** AWS::CloudWatch::MetricStream

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cloud-trail-cloud-watch-logs-enabled

Checks if AWS CloudTrail trails are configured to send logs to CloudWatch logs. The trail is NON_COMPLIANT if the CloudWatchLogsLogGroupArn property of the trail is empty.

**Identifier:** CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

**Resource Types:** AWS::CloudTrail::Trail

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

expectedDeliveryWindowAge (Optional), Type: int

Maximum age in hours of the most recent delivery to CloudWatch logs that satisfies compliance.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### cloudtrail-enabled

> **Important**
>
> For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different.

Checks if an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group.

**Identifier:** CLOUD_TRAIL_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

s3BucketName (Optional), Type: String

Name of S3 bucket for CloudTrail to deliver log files to.

snsTopicArn (Optional), Type: String

SNS topic ARN for CloudTrail to use for notifications.

cloudWatchLogsLogGroupArn (Optional), Type: String

CloudWatch log group ARN for CloudTrail to send data to.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### cloud-trail-encryption-enabled

Checks if AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) encryption. The rule is COMPLIANT if the KmsKeyId is defined.

**Identifier:** CLOUD_TRAIL_ENCRYPTION_ENABLED

**Resource Types:** AWS::CloudTrail::Trail

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### cloud-trail-log-file-validation-enabled

Checks if AWS CloudTrail creates a signed digest file with logs. AWS recommends that the file validation must be enabled on all trails. The rule is NON_COMPLIANT if the validation is not enabled.

**Identifier:** CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

**Resource Types:** AWS::CloudTrail::Trail

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cmk-backing-key-rotation-enabled

Checks if automatic key rotation is enabled for each key and matches to the key ID of the customer created AWS KMS key. The rule is NON_COMPLIANT if the AWS Config recorder role for a resource does not have the kms:DescribeKey permission.

> **Note**
>
> Automatic key rotation is not supported for asymmetric KMS keys, HMAC KMS keys, KMS keys with imported key material, or KMS keys in custom key stores.

**Identifier:** CMK_BACKING_KEY_ROTATION_ENABLED

**Resource Types:** AWS::KMS::Key

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-project-artifact-encryption

Checks if an AWS CodeBuild project has encryption enabled for all of its artifacts. The rule is NON_COMPLIANT if 'encryptionDisabled' is set to 'true' for any primary or secondary (if present) artifact configurations.

**Identifier:** CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

**Resource Types:** AWS::CodeBuild::Project

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-project-environment-privileged-check

Checks if an AWS CodeBuild project environment has privileged mode enabled. The rule is NON_COMPLIANT for a CodeBuild project if ‘privilegedMode’ is set to ‘true’.

**Identifier:** CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

**Resource Types:** AWS::CodeBuild::Project

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

exemptedProjects (Optional), Type: CSV

Comma-separated list of CodeBuild project names that are allowed to have 'privilegedMode' with value 'true'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-project-envvar-awscred-check

Checks if the project contains environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials.

**Identifier:** CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK

**Resource Types:** AWS::CodeBuild::Project

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-project-logging-enabled

Checks if an AWS CodeBuild project environment has at least one log option enabled. The rule is NON_COMPLIANT if the status of all present log configurations is set to 'DISABLED'.

**Identifier:** CODEBUILD_PROJECT_LOGGING_ENABLED

**Resource Types:** AWS::CodeBuild::Project

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

s3BucketNames (Optional), Type: String

Comma-separated list of Amazon S3 bucket names that logs should be sent to if S3 logs are configured.

cloudWatchGroupNames (Optional), Type: String

Comma-separated list of Amazon CloudWatch log group names that logs should be be sent to if CloudWatch logs are configured.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-project-s3-logs-encrypted

Checks if a AWS CodeBuild project configured with Amazon S3 Logs has encryption enabled for its logs. The rule is NON_COMPLIANT if ‘encryptionDisabled’ is set to ‘true’ in a S3LogsConfig of a CodeBuild project.

**Identifier:** CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

**Resource Types:** AWS::CodeBuild::Project

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

exemptedProjects (Optional), Type: CSV

Comma-separated list of CodeBuild project names that are allowed to output unencrypted logs.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-project-source-repo-url-check

Checks if the Bitbucket source repository URL contains sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't.

**Identifier:** CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

**Resource Types:** AWS::CodeBuild::Project

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-report-group-encrypted-at-rest

Checks if an AWS CodeBuild report group has encryption at rest setting enabled. The rule is NON_COMPLIANT if 'EncryptionDisabled' is 'true'.

**Identifier:** CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

**Resource Types:** AWS::CodeBuild::ReportGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codebuild-report-group-tagged

Checks if AWS CodeBuild report groups have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** CODEBUILD_REPORT_GROUP_TAGGED

**Resource Types:** AWS::CodeBuild::ReportGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codedeploy-auto-rollback-monitor-enabled

Checks if the deployment group is configured with automatic deployment rollback and deployment monitoring with alarms attached. The rule is NON_COMPLIANT if AutoRollbackConfiguration or AlarmConfiguration has not been configured or is not enabled.

**Identifier:** CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

**Resource Types:** AWS::CodeDeploy::DeploymentGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codedeploy-deployment-group-auto-rollback-enabled

Checks if AWS CodeDeploy deployment groups have auto rollback configuration enabled. The rule is NON_COMPLIANT if configuration.autoRollbackConfiguration.enabled is false or does not exist.

**Identifier:** CODEDEPLOY_DEPLOYMENT_GROUP_AUTO_ROLLBACK_ENABLED

**Resource Types:** AWS::CodeDeploy::DeploymentGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codedeploy-deployment-group-outdated-instances-update

Checks if AWS CodeDeploy deployment groups automatically update outdated instances. The rule is NON_COMPLIANT if configuration.outdatedInstancesStrategy is 'IGNORE'.

**Identifier:** CODEDEPLOY_DEPLOYMENT_GROUP_OUTDATED_INSTANCES_UPDATE

**Resource Types:** AWS::CodeDeploy::DeploymentGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codedeploy-ec2-minimum-healthy-hosts-configured

Checks if the deployment group for EC2/On-Premises Compute Platform is configured with a minimum healthy hosts fleet percentage or host count greater than or equal to the input threshold. The rule is NON_COMPLIANT if either is below the threshold.

**Identifier:** CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

**Resource Types:** AWS::CodeDeploy::DeploymentGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

minimumHealthyHostsFleetPercent (Optional), Type: int, Default: 66

Minimum percentage of healthy hosts fleet during deployment. Default value is set to 66 percent.

minimumHealthyHostsHostCount (Optional), Type: int, Default: 1

Minimum number of healthy hosts in fleet during deployment. Default value is set to 1.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codedeploy-lambda-allatonce-traffic-shift-disabled

Checks if the deployment group for Lambda Compute Platform is not using the default deployment configuration. The rule is NON_COMPLIANT if the deployment group is using the deployment configuration 'CodeDeployDefault.LambdaAllAtOnce'.

**Identifier:** CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

**Resource Types:** AWS::CodeDeploy::DeploymentGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codeguruprofiler-profiling-group-tagged

Checks if Amazon CodeGuru Profiler profiling groups have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** CODEGURUPROFILER_PROFILING_GROUP_TAGGED

**Resource Types:** AWS::CodeGuruProfiler::ProfilingGroup

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codegurureviewer-repository-association-tagged

Checks if Amazon CodeGuru Reviewer repository associations have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** CODEGURUREVIEWER_REPOSITORY_ASSOCIATION_TAGGED

**Resource Types:** AWS::CodeGuruReviewer::RepositoryAssociation

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codepipeline-deployment-count-check

Checks if the first deployment stage of AWS CodePipeline performs more than one deployment. Optionally checks if each of the subsequent remaining stages deploy to more than the specified number of deployments (`deploymentLimit`).

**Identifier:** CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

**Resource Types:** AWS::CodePipeline::Pipeline

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

deploymentLimit (Optional), Type: int

The maximum number of deployments each stage can perform.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## codepipeline-region-fanout-check

Checks if each stage in the AWS CodePipeline deploys to more than N times the number of the regions the AWS CodePipeline has deployed in all the previous combined stages, where N is the region fanout number. The first deployment stage can deploy to a maximum of one region and the second deployment stage can deploy to a maximum number specified in the `regionFanoutFactor`. If you do not provide a `regionFanoutFactor`, by default the value is three. For example: If 1st deployment stage deploys to one region and 2nd deployment stage deploys to three regions, 3rd deployment stage can deploy to 12 regions, that is, sum of previous stages multiplied by the region fanout (three) number. The rule is NON_COMPLIANT if the deployment is in more than one region in 1st stage or three regions in 2nd stage or 12 regions in 3rd stage.

**Identifier:** CODEPIPELINE_REGION_FANOUT_CHECK

**Resource Types:** AWS::CodePipeline::Pipeline

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

regionFanoutFactor (Optional), Type: int, Default: 3

The number of regions the AWS CodePipeline has deployed to in all previous stages is the acceptable number of regions any stage can deploy to.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-identity-pool-unauthenticated-logins

Checks if Amazon Cognito identity pools disallow unauthenticated logins. The rule is NON_COMPLIANT if configuration.AllowUnauthenticatedIdentities is true.

**Identifier:** COGNITO_IDENTITY_POOL_UNAUTHENTICATED_LOGINS

**Resource Types:** AWS::Cognito::IdentityPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-identity-pool-unauth-access-check

Checks if Amazon Cognito Identity Pool allows unauthenticated identities. The rule is NON_COMPLIANT if the Identity Pool is configured to allow unauthenticated identities.

**Identifier:** COGNITO_IDENTITY_POOL_UNAUTH_ACCESS_CHECK

**Resource Types:** AWS::Cognito::IdentityPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-userpool-cust-auth-threat-full-check

Checks if Amazon Cognito user pools have threat protection enabled with full-function enforcement mode for custom authentication. This rule is NON_COMPLIANT if threat protection for custom authentication is not set to full-function enforcement mode.

**Identifier:** COGNITO_USERPOOL_CUST_AUTH_THREAT_FULL_CHECK

**Resource Types:** AWS::Cognito::UserPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-user-pool-advanced-security-enabled

Checks if an Amazon Cognito user pool has advanced security enabled for standard authentication. The rule is NON_COMPLIANT if advanced security is not enabled. Optionally, you can specify an advanced security mode for the rule to check.

**Identifier:** COGNITO_USER_POOL_ADVANCED_SECURITY_ENABLED

**Resource Types:** AWS::Cognito::UserPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hong Kong), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

SecurityMode (Optional), Type: String

> String value of the advanced security mode for the rule to check. If provided, the rule is NON_COMPLIANT if the advanced security mode for user pools does not match this parameter value. Valid values are AUDIT and ENFORCED

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-user-pool-deletion-protection-enabled

Checks whether Amazon Cognito user pools has deletion protection enabled. This rule is NON_COMPLIANT if a user pool has deletion protection disabled.

**Identifier:** COGNITO_USER_POOL_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::Cognito::UserPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-user-pool-mfa-enabled

Checks if Amazon Cognito user pools configured with a PASSWORD-only sign-in policy have Multi-Factor Authentication (MFA) enabled. This rule is NON_COMPLIANT if the Cognito user pool configured with PASSWORD only sign in policy does not have MFA enabled.

**Identifier:** COGNITO_USER_POOL_MFA_ENABLED

**Resource Types:** AWS::Cognito::UserPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-user-pool-password-policy-check

Checks if the password policy for Amazon cognito user pool meets the specified requirements indicated in the parameters. The rule is NON_COMPLIANT if the user pool password policy does not meet the specified requirements.

**Identifier:** COGNITO_USER_POOL_PASSWORD_POLICY_CHECK

**Resource Types:** AWS::Cognito::UserPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requireSymbols (Optional), Type: boolean, Default: True

Whether to require at least one symbol in password.

temporaryPasswordValidity (Optional), Type: int, Default: 7

Number of days a temporary password remains valid.

minLength (Optional), Type: int, Default: 8

Minimum length required for user pool password.

requireNumbers (Optional), Type: boolean, Default: True

Whether to require at least one number in password.

requireUppercase (Optional), Type: boolean, Default: True

Whether to require at least one uppercase letter in password.

requireLowercase (Optional), Type: boolean, Default: True

Whether to require at least one lowercase letter in password.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cognito-user-pool-tagged

Checks if Amazon Cognito user pools have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** COGNITO_USER_POOL_TAGGED

**Resource Types:** AWS::Cognito::UserPool

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## connect-instance-logging-enabled

Checks if Amazon Connect instances have flow logs enabled in an Amazon CloudWatch log group. The rule is NON_COMPLIANT if an Amazon Connect instance does not have flow logs enabled.

**Identifier:** CONNECT_INSTANCE_LOGGING_ENABLED

**Resource Types:** AWS::Connect::Instance

**Trigger type:** Configuration changes

**AWS Region:** Only available in Africa (Cape Town), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## customerprofiles-domain-tagged

Checks if Amazon Connect Customer Profiles domains have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** CUSTOMERPROFILES_DOMAIN_TAGGED

**Resource Types:** AWS::CustomerProfiles::Domain

**Trigger type:** Configuration changes

**AWS Region:** Only available in Africa (Cape Town), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### customerprofiles-object-type-allow-profile-creation

Checks if Amazon Connect Customer Profiles object types allow the creation of a new standard profile if one does not exist. The rule is NON_COMPLIANT if configuration.AllowProfileCreation is false.

**Identifier:** CUSTOMERPROFILES_OBJECT_TYPE_ALLOW_PROFILE_CREATION

**Resource Types:** AWS::CustomerProfiles::ObjectType

**Trigger type:** Configuration changes

**AWS Region:** Only available in Africa (Cape Town), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### customerprofiles-object-type-tagged

Checks if Amazon Connect Customer Profiles object types have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** CUSTOMERPROFILES_OBJECT_TYPE_TAGGED

**Resource Types:** AWS::CustomerProfiles::ObjectType

**Trigger type:** Configuration changes

**AWS Region:** Only available in Africa (Cape Town), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## custom-eventbus-policy-attached

Checks if Amazon EventBridge custom event buses have a resource-based policy attached. The rule is NON_COMPLIANT if a custom event bus policy does not have an attached resource-based policy.

**Identifier:** CUSTOM_EVENTBUS_POLICY_ATTACHED

**Resource Types:** AWS::Events::EventBus

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## custom-schema-registry-policy-attached

Checks if custom Amazon EventBridge schema registries have a resource policy attached. The rule is NON_COMPLIANT for custom schema registries without a resource policy attached.

**Identifier:** CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

**Resource Types:** AWS::EventSchemas::Registry

**Trigger type:** Periodic

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), Asia Pacific (Hong Kong), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## cw-loggroup-retention-period-check

Checks if an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than `MinRetentionTime`, if specified, or else 365 days.

> **Note**
>
> If the retention setting is "Never expire" for a log group, the rule is marked as COMPLIANT.

**Identifier:** CW_LOGGROUP_RETENTION_PERIOD_CHECK

**Resource Types:** AWS::Logs::LogGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

LogGroupNames (Optional), Type: CSV

A comma-separated list of Log Group names to check the retention period.

MinRetentionTime (Optional), Type: int

Specify the retention time in days. Valid values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, and 3653. The default retention period is 365 days.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## datasync-location-object-storage-using-https

Checks if AWS DataSync location object storage servers use the HTTPS protocol to communicate. The rule is NON_COMPLIANT if configuration.ServerProtocol is not 'HTTPS'.

**Identifier:** DATASYNC_LOCATION_OBJECT_STORAGE_USING_HTTPS

**Resource Types:** AWS::DataSync::LocationObjectStorage

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## datasync-task-data-verification-enabled

Checks if AWS DataSync tasks have data verification enabled to perform additional verification at the end of your transfer. The rule is NON_COMPLIANT if configuration.Options.VerifyMode is 'NONE'.

**Identifier:** DATASYNC_TASK_DATA_VERIFICATION_ENABLED

**Resource Types:** AWS::DataSync::Task

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## datasync-task-logging-enabled

Checks if an AWS DataSync task has Amazon CloudWatch logging enabled. The rule is NON_COMPLIANT if an AWS DataSync task does not have Amazon CloudWatch logging enabled or if the logging level is not equivalent to the logging level that you specify.

**Identifier:** DATASYNC_TASK_LOGGING_ENABLED

**Resource Types:** AWS::DataSync::Task

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

logLevel (Optional), Type: String

String value for the logging level. Valid values include: 'BASIC' and 'TRANSFER'. If not specified, the default value is 'BASIC'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## datasync-task-tagged

Checks if AWS DataSync tasks have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** DATASYNC_TASK_TAGGED

**Resource Types:** AWS::DataSync::Task

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dax-encryption-enabled

Checks if Amazon DynamoDB Accelerator (DAX) clusters are encrypted. The rule is NON_COMPLIANT if a DAX cluster is not encrypted.

**Identifier:** DAX_ENCRYPTION_ENABLED

**Resource Types:** AWS::DAX::Cluster

**Trigger type:** Periodic

**AWS Region:** Only available in Europe (Stockholm), China (Beijing), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Europe (Spain), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dax-tls-endpoint-encryption

Checks if your Amazon DynamoDB Accelerator (DAX) cluster has ClusterEndpointEncryptionType set to TLS. The rule is NON_COMPLIANT if a DAX cluster is not encrypted by transport layer security (TLS).

**Identifier:** DAX_TLS_ENDPOINT_ENCRYPTION

**Resource Types:** AWS::DAX::Cluster

**Trigger type:** Periodic

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## db-instance-backup-enabled

Checks if RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window.

**Identifier:** DB_INSTANCE_BACKUP_ENABLED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

backupRetentionMinimum (Optional), Type: int

Minimum retention period for backups.

backupRetentionPeriod (Optional), Type: int

Retention period for backups.

checkReadReplicas (Optional), Type: boolean

Checks whether RDS DB instances have backups enabled for read replicas.

preferredBackupWindow (Optional), Type: String

Time range in which backups are created.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## desired-instance-tenancy

Checks EC2 instances for a 'tenancy' value. Also checks if AMI IDs are specified to be launched from those AMIs or if Host IDs are launched on those Dedicated Hosts. The rule is COMPLIANT if the instance matches a host and an AMI, if specified, in a list.

**Identifier:** DESIRED_INSTANCE_TENANCY

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

tenancy, Type: String

Desired tenancy of the instances. Valid values are DEDICATED, HOST and DEFAULT

imageId (Optional), Type: CSV

The rule evaluates instances launched only from AMIs with the specified IDs. Separate multiple AMI IDs with commas

hostId (Optional), Type: CSV

The IDs of the EC2 Dedicated Hosts on which the instances are meant to be launched. Separate multiple Host IDs with commas

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## desired-instance-type

Checks if your EC2 instances are of a specific instance type. The rule is NON_COMPLIANT if an EC2 instance is not specified in the parameter list. For a list of supported EC2 instance types, see Instance types in the EC2 User Guide for Linux Instances.

**Identifier:** DESIRED_INSTANCE_TYPE

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

instanceType, Type: CSV

Comma-separated list of EC2 instance types (for example, "t2.small, m4.large, i2.xlarge").

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-auto-minor-version-upgrade-check

Checks if an AWS Database Migration Service (AWS DMS) replication instance has automatic minor version upgrades enabled. The rule is NON_COMPLIANT if an AWS DMS replication instance is not configured with automatic minor version upgrades.

**Identifier:** DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

**Resource Types:** AWS::DMS::ReplicationInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS

GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-endpoint-ssl-configured

Checks if AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured.

**Context**: SSL/TLS connections provide one layer of security by encrypting data that moves between your client and a DB instance. Using server certificate provides an extra layer of security by validating that the connection is being made to an Amazon RDS DB instance. It does so by checking the server certificate that is automatically installed on all DB instances that you provision. By enabling SSL connection on AWS DMS, you protect the confidentiality of the data during the migration.

To configure SSL connection for AWS DMS, see Using SSL/TLS to encrypt a connection to a DB instance or cluster in the *Amazon Relational Database Service User Guide*.

**Identifier:** DMS_ENDPOINT_SSL_CONFIGURED

**Resource Types:** AWS::DMS::Endpoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-endpoint-tagged

Checks if AWS DMS endpoints have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** DMS_ENDPOINT_TAGGED

**Resource Types:** AWS::DMS::Endpoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-mongo-db-authentication-enabled

Checks if AWS Database Migration Service (AWS DMS) endpoints for MongoDb data stores are enabled for password-based authentication and access control. The rule is NON_COMPLIANT if password-based authentication and access control is not enabled.

**Identifier:** DMS_MONGO_DB_AUTHENTICATION_ENABLED

**Resource Types:** AWS::DMS::Endpoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-neptune-iam-authorization-enabled

Checks if an AWS Database Migration Service (AWS DMS) endpoint for Amazon Neptune databases is configured with IAM authorization. The rule is NON_COMPLIANT if an AWS DMS endpoint where Neptune is the target has IamAuthEnabled set to false.

**Identifier:** DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

**Resource Types:** AWS::DMS::Endpoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-redis-tls-enabled

Checks if AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL encryption is not enabled.

**Identifier:** DMS_REDIS_TLS_ENABLED

**Resource Types:** AWS::DMS::Endpoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-replication-instance-multi-az-enabled

Checks if AWS Database Migration Service (DMS) replication instances are configured with multiple Availability Zones. The rule is NON_COMPLIANT if a DMS replication instance is not configured to use multiple Availability Zones.

**Identifier:** DMS_REPLICATION_INSTANCE_MULTI_AZ_ENABLED

**Resource Types:** AWS::DMS::ReplicationInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-replication-not-public

Checks if AWS Database Migration Service (AWS DMS) replication instances are public. The rule is NON_COMPLIANT if PubliclyAccessible field is set to true.

**Identifier:** DMS_REPLICATION_NOT_PUBLIC

**Resource Types:** AWS::DMS::ReplicationInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-replication-task-sourcedb-logging

Checks if logging is enabled with a valid severity level for AWS DMS replication tasks of a source database. The rule is NON_COMPLIANT if logging is not enabled or logs for DMS replication tasks of a source database have a severity level that is not valid.

**Identifier:** DMS_REPLICATION_TASK_SOURCEDB_LOGGING

**Resource Types:** AWS::DMS::ReplicationTask

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-replication-task-tagged

Checks if AWS DMS replication tasks have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** DMS_REPLICATION_TASK_TAGGED

**Resource Types:** AWS::DMS::ReplicationTask

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific

(Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dms-replication-task-targetdb-logging

Checks if logging is enabled with a valid severity level for AWS DMS replication task events of a target database. The rule is NON_COMPLIANT if logging is not enabled or replication task logging of a target database has a severity level that is not valid.

**Identifier:** DMS_REPLICATION_TASK_TARGETDB_LOGGING

**Resource Types:** AWS::DMS::ReplicationTask

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## docdb-cluster-audit-logging-enabled

Checks if an Amazon DocumentDB (with MongoDB compatibility) instance cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if an Amazon DocumentDB instance cluster does not have CloudWatch log export enabled for audit logs.

**Identifier:** DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Stockholm), Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), US West (N. California), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## docdb-cluster-backup-retention-check

Checks if an Amazon Document DB cluster retention period is set to specific number of days. The rule is NON_COMPLIANT if the retention period is less than the value specified by the parameter.

**Identifier:** DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Stockholm), Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-

West), Mexico (Central), US West (N. California), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

minimumBackupRetentionPeriod (Optional), Type: int

Minimum days backups should be kept. Valid values 1 to 35, default value is 7. This rule is NON_COMPLIANT if value is greater than 'backupRetentionPeriod'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## docdb-cluster-deletion-protection-enabled

Checks if an Amazon DocumentDB (with MongoDB compatibility) cluster has deletion protection enabled. The rule is NON_COMPLIANT if an Amazon DocumentDB cluster has the deletionProtection field set to false.

**Identifier:** DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Stockholm), Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), US West (N. California), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## docdb-cluster-encrypted

Checks if storage encryption is enabled for your Amazon DocumentDB (with MongoDB compatibility) clusters. The rule is NON_COMPLIANT if storage encryption is not enabled.

**Identifier:** DOCDB_CLUSTER_ENCRYPTED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Stockholm), Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), US West (N. California), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

A comma-separated list of KMS key ARNs to compare with the KmsKeyID of the encrypted cluster.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## docdb-cluster-encrypted-in-transit

Checks if connections to Amazon DocumentDB clusters are configured to use encryption in transit. The rule is NON_COMPLIANT if the parameter group is not "in-sync", or the TLS parameter is set to either "disabled" or a value in `excludeTlsParameters`.

**Identifier:** DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Europe (Stockholm), Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), US West (N. California), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

excludeTlsParameters (Optional), Type: CSV

Comma-separated list of TLS cluster parameters for the rule to NOT check. Default value: 'disabled'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## docdb-cluster-snapshot-public-prohibited

Checks if Amazon DocumentDB manual cluster snapshots are public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public.

**Identifier:** DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

**Resource Types:** AWS::RDS::DBClusterSnapshot

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Middle East (UAE), Europe (Frankfurt), South America (Sao Paulo), Asia Pacific (Hong Kong), Asia Pacific (Hyderabad), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Europe (Milan), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-autoscaling-enabled

Checks if Amazon DynamoDB tables or global secondary indexes can process read/write capacity using on-demand mode or provisioned mode with auto scaling enabled. The rule is NON_COMPLIANT if either mode is used without auto scaling enabled

**Identifier:** DYNAMODB_AUTOSCALING_ENABLED

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

minProvisionedReadCapacity (Optional), Type: int

The minimum number of units that should be provisioned with read capacity in the Auto Scaling group.

maxProvisionedReadCapacity (Optional), Type: int

The maximum number of units that should be provisioned with read capacity in the Auto Scaling group.

targetReadUtilization (Optional), Type: double

The target utilization percentage for read capacity. Target utilization is expressed in terms of the ratio of consumed capacity to provisioned capacity.

minProvisionedWriteCapacity (Optional), Type: int

The minimum number of units that should be provisioned with write capacity in the Auto Scaling group.

maxProvisionedWriteCapacity (Optional), Type: int

The maximum number of units that should be provisioned with write capacity in the Auto Scaling group.

targetWriteUtilization (Optional), Type: double

The target utilization percentage for write capacity. Target utilization is expressed in terms of the ratio of consumed capacity to provisioned capacity.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### dynamodb-in-backup-plan

Checks whether Amazon DynamoDB table is present in AWS Backup Plans. The rule is NON_COMPLIANT if Amazon DynamoDB tables are not present in any AWS Backup plan.

**Identifier:** DYNAMODB_IN_BACKUP_PLAN

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### dynamodb-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon DynamoDB Tables within the specified period. The rule is NON_COMPLIANT if the DynamoDB Table does not have a corresponding recovery point created within the specified time period.

**Identifier:** DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of the DynamoDB Tables for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

Name of DynamoDB Table for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-meets-restore-time-target

Checks if the restore time of Amazon DynamoDB Tables meets the specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of a DynamoDB Table is greater than maxRestoreTime minutes.

**Identifier:** DYNAMODB_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags of the DynamoDB Tables for the rule to check, in JSON format.

resourceId (Optional), Type: String

Name of DynamoDB Table for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-pitr-enabled

Checks if point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables.

**Identifier:** DYNAMODB_PITR_ENABLED

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-resources-protected-by-backup-plan

Checks if Amazon DynamoDB tables are protected by a backup plan. The rule is NON_COMPLIANT if the DynamoDB Table is not covered by a backup plan.

**Identifier:** DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for DynamoDB tables for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

Name of DynamoDB table for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-table-deletion-protection-enabled

Checks if an Amazon DynamoDB table have deletion protection set to enabled. The rule is NON_COMPLIANT if the table have deletion protection set to disabled.

**Identifier:** DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-table-encrypted-kms

Checks if Amazon DynamoDB table is encrypted with AWS Key Management Service (KMS). The rule is NON_COMPLIANT if Amazon DynamoDB table is not encrypted with AWS KMS. The rule

is also NON_COMPLIANT if the encrypted AWS KMS key is not present in `kmsKeyArns` input parameter.

**Identifier:** DYNAMODB_TABLE_ENCRYPTED_KMS

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma separated list of AWS KMS key ARNs allowed for encrypting Amazon DynamoDB Tables

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-table-encryption-enabled

Checks if the Amazon DynamoDB tables are encrypted and checks their status. The rule is COMPLIANT if the status is enabled or enabling.

**Identifier:** DYNAMODB_TABLE_ENCRYPTION_ENABLED

**Resource Types:** AWS::DynamoDB::Table

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## dynamodb-throughput-limit-check

Checks if provisioned DynamoDB throughput is approaching the maximum limit for your account. By default, the rule checks if provisioned throughput exceeds a threshold of 80 percent of your account limits.

**Identifier:** DYNAMODB_THROUGHPUT_LIMIT_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

accountRCUThresholdPercentage (Optional), Type: int, Default: 80

Percentage of provisioned read capacity units for your account. When this value is reached, the rule is marked as noncompliant.

accountWCUThresholdPercentage (Optional), Type: int, Default: 80

Percentage of provisioned write capacity units for your account. When this value is reached, the rule is marked as noncompliant.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ebs-in-backup-plan

Check if Amazon Elastic Block Store (Amazon EBS) volumes are added in backup plans of AWS Backup. The rule is NON_COMPLIANT if Amazon EBS volumes are not included in backup plans.

**Identifier:** EBS_IN_BACKUP_PLAN

**Resource Types:** AWS::EC2::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ebs-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon Elastic Block Store (Amazon EBS). The rule is NON_COMPLIANT if the Amazon EBS volume does not have a corresponding recovery point created within the specified time period.

**Identifier:** EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::EC2::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon EBS volumes for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Amazon EBS volume for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ebs-meets-restore-time-target

Checks if the restore time of Amazon Elastic Block Store (Amazon EBS) volumes meets the specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of an Amazon EBS volume is greater than maxRestoreTime minutes.

**Identifier:** EBS_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::EC2::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags for Amazon EBS volumes for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Amazon EBS volume for the rule to check.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### ebs-optimized-instance

Checks if Amazon EBS optimization is enabled for your Amazon Elastic Compute Cloud (Amazon EC2) instances that can be Amazon EBS-optimized. The rule is NON_COMPLIANT if EBS optimization is not enabled for an Amazon EC2 instance that can be EBS-optimized.

> **Note**
>
> EC2 instances which are EBS-optimized by default always result in rule evaluations returning `COMPLIANT`.

**Identifier:** EBS_OPTIMIZED_INSTANCE

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ebs-resources-in-logically-air-gapped-vault

Checks if Amazon Elastic Block Store (Amazon EBS) volumes are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon EBS volume is not in a logically air-gapped vault within the specified time period.

**Identifier:** EBS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

**Resource Types:** AWS::EC2::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon EBS volumes for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Amazon EBS volume for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 2184 for hours, 91 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ebs-resources-protected-by-backup-plan

Checks if Amazon Elastic Block Store (Amazon EBS) volumes are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon EBS volume is not covered by a backup plan.

**Identifier:** EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::EC2::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for Amazon EBS volumes for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Amazon EBS volume for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ebs-snapshot-block-public-access

Checks if block public access is enabled for Amazon EBS snapshots in an AWS Region. The rule is NON_COMPLIANT if block public access is not enabled for all public sharing of EBS snapshots in an AWS Region.

**Identifier:** EBS_SNAPSHOT_BLOCK_PUBLIC_ACCESS

**Resource Types:** AWS::EC2::SnapshotBlockPublicAccess

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ebs-snapshot-public-restorable-check

Checks if Amazon Elastic Block Store (Amazon EBS) snapshots are not publicly restorable. The rule is NON_COMPLIANT if one or more snapshots with RestorableByUserIds field are set to all, that is, Amazon EBS snapshots are public.

**Identifier:** EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Europe (Spain) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-capacity-reservation-tagged

Checks if Amazon EC2 capacity reservations have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_CAPACITY_RESERVATION_TAGGED

**Resource Types:** AWS::EC2::CapacityReservation

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-carrier-gateway-tagged

Checks if Amazon EC2 carrier gateways have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_CARRIER_GATEWAY_TAGGED

**Resource Types:** AWS::EC2::CarrierGateway

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-client-vpn-connection-log-enabled

Checks if AWS Client VPN endpoint has client connection logging enabled. The rule is NON_COMPLIANT if 'Configuration.ConnectionLogOptions.Enabled' is set to false.

**Identifier:** EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

**Resource Types:** AWS::EC2::ClientVpnEndpoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-client-vpn-endpoint-tagged

Checks if Amazon EC2 client VPN endpoints have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_CLIENT_VPN_ENDPOINT_TAGGED

**Resource Types:** AWS::EC2::ClientVpnEndpoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-client-vpn-not-authorize-all

Checks if the AWS Client VPN authorization rules authorizes connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true.

**Identifier:** EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

**Resource Types:** AWS::EC2::ClientVpnEndpoint

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-dhcp-options-tagged

Checks if Amazon EC2 DHCP options have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_DHCP_OPTIONS_TAGGED

**Resource Types:** AWS::EC2::DHCPOptions

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-ebs-encryption-by-default

Checks if Amazon Elastic Block Store (EBS) encryption is enabled by default. The rule is NON_COMPLIANT if the encryption is not enabled.

**Identifier:** EC2_EBS_ENCRYPTION_BY_DEFAULT

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-enis-source-destination-check-enabled

Checks if EC2 ENIs managed by users have source/destination check enabled. The rule is NON_COMPLIANT if source/destination check is disabled on these ENIs for 'lambda', 'aws_codestar_connections_managed', 'branch', 'efa', 'interface', and 'quicksight'.

**Identifier:** EC2_ENIS_SOURCE_DESTINATION_CHECK_ENABLED

**Resource Types:** AWS::EC2::NetworkInterface

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-fleet-tagged

Checks if Amazon EC2 fleets have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_FLEET_TAGGED

**Resource Types:** AWS::EC2::EC2Fleet

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-imdsv2-check

Checks whether your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON_COMPLIANT if the HttpTokens is set to optional.

**Identifier:** EC2_IMDSV2_CHECK

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-instance-detailed-monitoring-enabled

Checks if detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled.

**Identifier:** EC2_INSTANCE_DETAILED_MONITORING_ENABLED

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-instance-launched-with-allowed-ami

Checks if running or stopped EC2 instances were launched with Amazon Machine Images (AMIs) that meet your Allowed AMIs criteria. The rule is NON_COMPLIANT if an AMI doesn't meet the Allowed AMIs criteria and the Allowed AMIs settings isn't disabled.

**Identifier:** EC2_INSTANCE_LAUNCHED_WITH_ALLOWED_AMI

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

InstanceStateNameList (Optional), Type: CSV

Comma-separate list of Amazon EC2 instance states for the rule to check. Valid values are "running" and "stopped".

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-instance-managed-by-systems-manager

> **Important**
>
> For this rule, the rule identifier (EC2_INSTANCE_MANAGED_BY_SSM) and rule name (ec2-instance-managed-by-systems-manager) are different.

Checks if your Amazon EC2 instances are managed by AWS Systems Manager Agent (SSM Agent). The rule is NON_COMPLIANT if an EC2 instance is running and the SSM Agent is stopped, or if an EC2 instance is running and the SSM Agent is terminated.

> **Note**
>
> The rule will not return NON_COMPLIANT if an EC2 instance is stopped and the SSM Agent is running.

**Identifier:** EC2_INSTANCE_MANAGED_BY_SSM

**Resource Types:** AWS::EC2::Instance, AWS::SSM::ManagedInstanceInventory

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-instance-multiple-eni-check

Checks if Amazon Elastic Compute Cloud (Amazon EC2) uses multiple Elastic Network Interfaces (ENIs) or Elastic Fabric Adapters (EFAs). The rule is NON_COMPLIANT an Amazon EC2 instance use multiple network interfaces.

**Identifier:** EC2_INSTANCE_MULTIPLE_ENI_CHECK

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

NetworkInterfaceIds (Optional), Type: CSV

Comma-separated list of network instance IDs

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-instance-no-public-ip

Checks whether Amazon Elastic Compute Cloud (Amazon EC2) instances have a public IP association. The rule is NON_COMPLIANT if the publicIp field is present in the Amazon EC2 instance configuration item. This rule applies only to IPv4.

**Context**: Public IP addresses can make EC2 instances directly accessible from the internet, which might not always be desirable from a security or compliance standpoint:

- **Security**: In many cases, you might not want your EC2 instances to have public IP addresses unless they need to be publicly accessible. Having a public IP address can expose your EC2 instance to potential security risks, such as unauthorized access or attacks.
- **Compliance**: Various compliance standards such as PCI, DSS, or HIPAA have specific requirements regarding network segmentation and access controls. Ensuring that EC2 instances do not have unnecessary public IP addresses can help ensure compliance with these requirements.
- **Cost Management**: Public IP addresses can incur additional costs, especially if there are EC2 instances continuously associated with them. By identifying EC2 instances with public IPs which do not need them, you can potentially reduce costs.

**Identifier:** EC2_INSTANCE_NO_PUBLIC_IP

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-instance-profile-attached

Checks if an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance.

**Identifier:** EC2_INSTANCE_PROFILE_ATTACHED

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), China (Ningxia) Region

**Parameters:**

IamInstanceProfileArnList (Optional), Type: CSV

Comma-separated list of IAM profile Amazon Resource Names (ARNs) that can be attached to Amazon EC2 instances.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon Elastic Compute Cloud (Amazon EC2) instances. The rule is NON_COMPLIANT if the Amazon EC2 instance does not have a corresponding recovery point created within the specified time period.

**Identifier:** EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon EC2 instances for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Amazon EC2 instance for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-launch-templates-ebs-volume-encrypted

Checks whether Amazon EC2 launch templates have encryption enabled for all attached EBS volumes.The rule is NON_COMPLIANT if encryption is set to False for any EBS volume configured in the launch template.

**Identifier:** EC2_LAUNCH_TEMPLATES_EBS_VOLUME_ENCRYPTED

**Resource Types:** AWS::EC2::LaunchTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-launch-template-imdsv2-check

Checks if the currently set default version of an Amazon EC2 Launch Template requires new launched instances to use V2 of the Amazon EC2 Instance Metadata Service (IMDSv2). The rule is NON_COMPLIANT if 'Metadata version' is not specified as V2 (IMDSv2).

**Identifier:** EC2_LAUNCH_TEMPLATE_IMDSV2_CHECK

**Resource Types:** AWS::EC2::LaunchTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-launch-template-public-ip-disabled

Checks if Amazon EC2 Launch Templates are set to assign public IP addresses to Network Interfaces. The rule is NON_COMPLIANT if the default version of an EC2 Launch Template has at least 1 Network Interface with 'AssociatePublicIpAddress' set to 'true'.

**Identifier:** EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

**Resource Types:** AWS::EC2::LaunchTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS

GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

exemptedLaunchTemplates (Optional), Type: CSV

Comma-separated list of exempted EC2 Launch Template IDs that are allowed to have Network Interfaces with the AssociatePublicIpAddress value set to 'true'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-launch-template-tagged

Checks if Amazon EC2 launch templates have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_LAUNCH_TEMPLATE_TAGGED

**Resource Types:** AWS::EC2::LaunchTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-managedinstance-applications-blacklisted

Checks if none of the specified applications are installed on the instance. Optionally, specify the version. Newer versions will not be denylisted. Optionally, specify the platform to apply the rule only to instances running that platform.

**Identifier:** EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

**Resource Types:** AWS::SSM::ManagedInstanceInventory

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

applicationNames, Type: CSV

Comma-separated list of application names. Optionally, specify versions appended with ':' (for example, 'Chrome:0.5.3, Firefox').

> **Note**
>
> The application names must be an exact match. For example, use **`firefox`** on Linux or **`firefox-compat`** on Amazon Linux. In addition, AWS Config does not currently support wildcards for the *applicationNames* parameter (for example, **`firefox*`**).

platformType (Optional), Type: String

Platform type (for example, 'Linux' or 'Windows').

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-managedinstance-applications-required

Checks if all of the specified applications are installed on the instance. Optionally, specify the minimum acceptable version. You can also specify the platform to apply the rule only to instances running that platform.

> **Note**
>
> Ensure that SSM agent is running on the EC2 instance and an association to gather application software inventory is created. The rule returns `NOT_APPLICABLE` if SSM agent is not installed or an association is not yet created or running.

**Identifier:** EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

**Resource Types:** AWS::SSM::ManagedInstanceInventory

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

applicationNames, Type: CSV

Comma-separated list of application names. Optionally, specify versions appended with ':' (for example, 'Chrome:0.5.3, Firefox').

> **Note**
>
> The application names must be an exact match. For example, use **`firefox`** on Linux or **`firefox-compat`** on Amazon Linux. In addition, AWS Config does not currently support wildcards for the *applicationNames* parameter (for example, **`firefox*`**).

platformType (Optional), Type: String

Platform type (for example, 'Linux' or 'Windows').

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-managedinstance-association-compliance-status-check

Checks if the status of the AWS Systems Manager association compliance is COMPLIANT or NON_COMPLIANT after the association execution on the instance. The rule is compliant if the field status is COMPLIANT. For more information about associations, see What is an association?.

**Identifier:** EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

**Resource Types:** AWS::SSM::AssociationCompliance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Osaka), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-managedinstance-inventory-blacklisted

Checks whether instances managed by Amazon EC2 Systems Manager are configured to collect blacklisted inventory types.

**Identifier:** EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

**Resource Types:** AWS::SSM::ManagedInstanceInventory

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

inventoryNames, Type: CSV

Comma separated list of Systems Manager inventory types (for example, 'AWS:Network, AWS:WindowsUpdate').

platformType (Optional), Type: String

Platform type (for example, 'Linux').

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-managedinstance-patch-compliance-status-check

Checks if the compliance status of the AWS Systems Manager patch compliance is COMPLIANT or NON_COMPLIANT after the patch installation on the instance. The rule is compliant if the field status is COMPLIANT.

**Identifier:** EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

**Resource Types:** AWS::SSM::PatchCompliance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Osaka), Europe (Milan), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-managedinstance-platform-check

Checks whether EC2 managed instances have the desired configurations.

**Identifier:** EC2_MANAGEDINSTANCE_PLATFORM_CHECK

**Resource Types:** AWS::SSM::ManagedInstanceInventory

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

platformType, Type: String

Platform type (for example, 'Linux').

platformVersion (Optional), Type: String

Platform version (for example, '2016.09').

agentVersion (Optional), Type: String

Agent version (for example, '2.0.433.0').

platformName (Optional), Type: String

The version of the platform (for example, '2016.09')

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-meets-restore-time-target

Checks if the restore time of Amazon Elastic Compute Cloud (Amazon EC2) instances meets the specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of an Amazon EC2 instance is greater than maxRestoreTime minutes.

**Identifier:** EC2_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags of Amazon EC2 instances for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Amazon EC2 instance for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-network-insights-access-scope-analysis-tagged

Checks if Amazon EC2 network insights access scope analyses have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_NETWORK_INSIGHTS_ACCESS_SCOPE_ANALYSIS_TAGGED

**Resource Types:** AWS::EC2::NetworkInsightsAccessScopeAnalysis

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-network-insights-access-scope-tagged

Checks if Amazon EC2 network insights access scopes have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_NETWORK_INSIGHTS_ACCESS_SCOPE_TAGGED

**Resource Types:** AWS::EC2::NetworkInsightsAccessScope

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-network-insights-analysis-tagged

Checks if Amazon EC2 network insights analyses have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_NETWORK_INSIGHTS_ANALYSIS_TAGGED

**Resource Types:** AWS::EC2::NetworkInsightsAnalysis

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-network-insights-path-tagged

Checks if Amazon EC2 network insights paths have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_NETWORK_INSIGHTS_PATH_TAGGED

**Resource Types:** AWS::EC2::NetworkInsightsPath

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-no-amazon-key-pair

Checks if running Amazon Elastic Compute Cloud (EC2) instances are launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair.

**Identifier:** EC2_NO_AMAZON_KEY_PAIR

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-paravirtual-instance-check

Checks if the virtualization type of an EC2 instance is paravirtual. This rule is NON_COMPLIANT for an EC2 instance if 'virtualizationType' is set to 'paravirtual'.

**Identifier:** EC2_PARAVIRTUAL_INSTANCE_CHECK

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** Only available in China (Beijing), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-prefix-list-tagged

Checks if Amazon EC2 managed prefix lists have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_PREFIX_LIST_TAGGED

**Resource Types:** AWS::EC2::PrefixList

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-resources-in-logically-air-gapped-vault

Checks if Amazon Elastic Compute Cloud (Amazon EC2) instances are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon EC2 instance is not in a logically air-gapped vault within the specified time period.

**Identifier:** EC2_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon EC2 instances for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Amazon EC2 instance for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 2184 for hours, 91 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-resources-protected-by-backup-plan

Checks if Amazon Elastic Compute Cloud (Amazon EC2) instances are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon EC2 instance is not covered by a backup plan.

> **Note**
>
> This rule is only applicable to running Amazon EC2 instances and not to instances that are powered down.

**Identifier:** EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for Amazon EC2 instances for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Amazon EC2 instance for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-security-group-attached-to-eni

Checks that non-default security groups are attached to Amazon Elastic Compute Cloud (EC2) instances or an elastic network interfaces (ENIs). The rule returns NON_COMPLIANT if the security group is not associated with an EC2 instance or an ENI.

**Identifier:** EC2_SECURITY_GROUP_ATTACHED_TO_ENI

**Resource Types:** AWS::EC2::SecurityGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (UAE), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-security-group-attached-to-eni-periodic

Checks if non-default security groups are attached to Elastic network interfaces (ENIs). The rule is NON_COMPLIANT if the security group is not associated with an ENI. Security groups not owned by the calling account evaluate as NOT_APPLICABLE.

> **Note**
>
> This rule reports on the `AWS::EC2::SecurityGroup` resource type. However, in order for the rule to run effectively, you must enable the recording of the `AWS::EC2::NetworkInterface` resource type.

**Identifier:** EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

**Resource Types:** AWS::EC2::SecurityGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-spot-fleet-request-ct-encryption-at-rest

Checks if Amazon EC2 Spot Fleet request launch parameters set encrypted to True for attached EBS volumes. The rule is NON_COMPLIANT if any EBS volumes has encrypted set to False. The rule does not evaluate spot fleet requests using launch templates.

**Identifier:** EC2_SPOT_FLEET_REQUEST_CT_ENCRYPTION_AT_REST

**Resource Types:** AWS::EC2::SpotFleet

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Ireland), US East (N. Virginia), Asia Pacific (Seoul), US West (Oregon), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-stopped-instance

Checks if there are Amazon Elastic Compute Cloud (Amazon EC2) instances stopped for more than the allowed number of days. The rule is NON_COMPLIANT if the state of an Amazon EC2 instance has been stopped for longer than the allowed number of days, or if the amount of time cannot be determined.

**Identifier:** EC2_STOPPED_INSTANCE

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

AllowedDays (Optional), Type: int, Default: 30

The number of days an Amazon EC2 instance can be stopped before the rule is NON_COMPLIANT. The default number of days is 30.

> **Note**
>
> The number of days selected needs to be less than the configured retention period since this rule relies on the historical data collected. For more information about historical data retention, see Deleting AWS Config Data.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-token-hop-limit-check

Checks if an Amazon Elastic Compute Cloud (EC2) instance metadata has a specified token hop limit that is below the desired limit. The rule is NON_COMPLIANT for an instance if it has a hop limit value above the intended limit.

**Identifier:** EC2_TOKEN_HOP_LIMIT_CHECK

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

tokenHopLimit (Optional), Type: int

The desired token hop limit. Valid values are between 1 and 64, both inclusive. Default value is 1 if parameter is not specified.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-traffic-mirror-filter-description

Checks if Amazon EC2 traffic mirror filters have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** EC2_TRAFFIC_MIRROR_FILTER_DESCRIPTION

**Resource Types:** AWS::EC2::TrafficMirrorFilter

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-traffic-mirror-filter-tagged

Checks if Amazon EC2 traffic mirror filters have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_TRAFFIC_MIRROR_FILTER_TAGGED

**Resource Types:** AWS::EC2::TrafficMirrorFilter

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-traffic-mirror-session-description

Checks if Amazon EC2 traffic mirror sessions have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** EC2_TRAFFIC_MIRROR_SESSION_DESCRIPTION

**Resource Types:** AWS::EC2::TrafficMirrorSession

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-traffic-mirror-session-tagged

Checks if Amazon EC2 traffic mirror sessions have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_TRAFFIC_MIRROR_SESSION_TAGGED

**Resource Types:** AWS::EC2::TrafficMirrorSession

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-traffic-mirror-target-description

Checks if Amazon EC2 traffic mirror targets have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** EC2_TRAFFIC_MIRROR_TARGET_DESCRIPTION

**Resource Types:** AWS::EC2::TrafficMirrorTarget

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-traffic-mirror-target-tagged

Checks if Amazon EC2 traffic mirror targets have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_TRAFFIC_MIRROR_TARGET_TAGGED

**Resource Types:** AWS::EC2::TrafficMirrorTarget

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-transit-gateway-auto-vpc-attach-disabled

Checks if Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways have 'AutoAcceptSharedAttachments' enabled. The rule is NON_COMPLIANT for a Transit Gateway if 'AutoAcceptSharedAttachments' is set to 'enable'.

**Identifier:** EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

**Resource Types:** AWS::EC2::TransitGateway

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-transit-gateway-multicast-domain-tagged

Checks if Amazon EC2 transit gateway multicast domains have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_TRANSIT_GATEWAY_MULTICAST_DOMAIN_TAGGED

**Resource Types:** AWS::EC2::TransitGatewayMulticastDomain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-volume-inuse-check

Checks if EBS volumes are attached to EC2 instances. Optionally checks if EBS volumes are marked for deletion when an instance is terminated.

The rule is COMPLIANT if an EBS volume is attached to running or stopped EC2 instances.

The rule is NON_COMPLIANT if an EBS volume is not attached to any EC2 instance or is attached to a terminated EC2 instance.

**Identifier:** EC2_VOLUME_INUSE_CHECK

**Resource Types:** AWS::EC2::Volume

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), China (Ningxia) Region

**Parameters:**

deleteOnTermination (Optional), Type: boolean

EBS volumes are marked for deletion when an instance is terminated. Possible values: True or False (other input values are marked as NON_COMPLIANT). If set to `True`, the rule is NON_COMPLIANT if a terminated EBS volume is not marked for deletion.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-vpn-connection-logging-enabled

Checks if AWS Site-to-Site VPN connections have Amazon CloudWatch logging enabled for both tunnels. The rule is NON_COMPLIANT if a Site-to-Site VPN connection does not have CloudWatch logging enabled for either or both tunnels.

**Identifier:** EC2_VPN_CONNECTION_LOGGING_ENABLED

**Resource Types:** AWS::EC2::VPNConnection

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ec2-vpn-connection-tagged

Checks if Amazon EC2 VPN connections have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EC2_VPN_CONNECTION_TAGGED

**Resource Types:** AWS::EC2::VPNConnection

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecr-private-image-scanning-enabled

Checks if a private Amazon Elastic Container Registry (Amazon ECR) repository has image scanning enabled. The rule is NON_COMPLIANT if the private Amazon ECR repository's scan frequency is not on scan on push or continuous scan. For more information on enabling image scanning, see Image scanning in the *Amazon ECR User Guide*.

**Identifier:** ECR_PRIVATE_IMAGE_SCANNING_ENABLED

**Resource Types:** AWS::ECR::Repository

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecr-private-lifecycle-policy-configured

Checks if a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository.

**Identifier:** ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

**Resource Types:** AWS::ECR::Repository

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecr-private-tag-immutability-enabled

Checks if a private Amazon Elastic Container Registry (ECR) repository has tag immutability enabled. This rule is NON_COMPLIANT if tag immutability is not enabled for the private ECR repository.

**Identifier:** ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

**Resource Types:** AWS::ECR::Repository

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecr-repository-cmk-encryption-enabled

Checks if ECR repository is encrypted at rest using customer-managed KMS key. This rule is NON_COMPLIANT if the repository is encrypted using AES256 or the default KMS key ('aws/ecr').

**Identifier:** ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

**Resource Types:** AWS::ECR::Repository

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

> Comma-separated list of KMS key Amazon Resource Names (ARNs) intended to encrypt the ECR repository.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecr-repository-tagged

Checks if Amazon ECR repositories have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ECR_REPOSITORY_TAGGED

**Resource Types:** AWS::ECR::Repository

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-awsvpc-networking-enabled

Checks if the networking mode for active ECSTaskDefinitions is set to ‘awsvpc’. This rule is NON_COMPLIANT if active ECSTaskDefinitions is not set to ‘awsvpc’.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_AWSVPC_NETWORKING_ENABLED

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-capacity-provider-tagged

Checks if Amazon ECS capacity providers have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ECS_CAPACITY_PROVIDER_TAGGED

**Resource Types:** AWS::ECS::CapacityProvider

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### ecs-capacity-provider-termination-check

Checks if an Amazon ECS Capacity provider containing Auto Scaling groups has managed termination protection enabled. This rule is NON_COMPLIANT if managed termination protection is disabled on the ECS Capacity Provider.

**Identifier:** ECS_CAPACITY_PROVIDER_TERMINATION_CHECK

**Resource Types:** AWS::ECS::CapacityProvider

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### ecs-containers-nonprivileged

Checks if the privileged parameter in the container definition of ECSTaskDefinitions is set to 'true'. The rule is NON_COMPLIANT if the privileged parameter is 'true'.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_CONTAINERS_NONPRIVILEGED

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### ecs-containers-readonly-access

Checks if Amazon Elastic Container Service (Amazon ECS) Containers only have read-only access to its root filesystems. The rule is NON_COMPLIANT if the readonlyRootFilesystem parameter in the container definition of ECSTaskDefinitions is set to 'false'.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_CONTAINERS_READONLY_ACCESS

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-container-insights-enabled

Checks if Amazon Elastic Container Service clusters have container insights enabled. The rule is NON_COMPLIANT if container insights are not enabled.

**Identifier:** ECS_CONTAINER_INSIGHTS_ENABLED

**Resource Types:** AWS::ECS::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-fargate-latest-platform-version

Checks if ECS Fargate services is set to the latest platform version. The rule is NON_COMPLIANT if PlatformVersion for the Fargate launch type is not set to LATEST, or if neither latestLinuxVersion nor `latestWindowsVersion` are provided as parameters.

**Identifier:** ECS_FARGATE_LATEST_PLATFORM_VERSION

**Resource Types:** AWS::ECS::Service

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

latestLinuxVersion (Optional), Type: String

Latest Linux supported 'PlatformVersion' in semantic versioning (SemVer) format. Parameter may be needed if Fargate was deployed and the 'PlatformVersion' was explicitly specified or CodeDeploy is used as the 'DeploymentController'

latestWindowsVersion (Optional), Type: String

Latest Windows supported 'PlatformVersion' in semantic versioning (SemVer) format. Parameter may be needed if Fargate was deployed and the 'PlatformVersion' was explicitly specified or CodeDeploy is used as the 'DeploymentController'

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-no-environment-secrets

Checks if secrets are passed as container environment variables. The rule is NON_COMPLIANT if 1 or more environment variable key matches a key listed in the '`secretKeys`' parameter (excluding environmental variables from other locations such as Amazon S3).

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_NO_ENVIRONMENT_SECRETS

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

secretKeys, Type: CSV

Comma-separated list of key names to search for in the environment variables of container definitions within Task Definitions. Extra spaces will be removed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### ecs-task-definition-efs-encryption-enabled

Checks if Amazon ECS Task Definitions with EFS volumes have in-transit encryption enabled. The rule is NON_COMPLIANT if an ECS Task Definition contains an EFS volume without transit encryption enabled.

**Identifier:** ECS_TASK_DEFINITION_EFS_ENCRYPTION_ENABLED

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### ecs-task-definition-linux-user-non-root

Checks if the latest active revision of an Amazon ECS task definition configures Linux containers to run as non-root users.The rule is NON_COMPLIANT if root user is specified or user configuration is absent for any container.

**Identifier:** ECS_TASK_DEFINITION_LINUX_USER_NON_ROOT

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-task-definition-log-configuration

Checks if logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_TASK_DEFINITION_LOG_CONFIGURATION

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-task-definition-memory-hard-limit

Checks if Amazon Elastic Container Service (ECS) task definitions have a set memory limit for its container definitions. The rule is NON_COMPLIANT for a task definition if the 'memory' parameter is absent for one container definition.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-task-definition-network-mode-not-host

Checks if the latest active revision of Amazon ECS task definitions use host network mode. The rule is NON_COMPLIANT if the latest active revision of the ECS task definition uses host network mode.

**Identifier:** ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-task-definition-nonroot-user

Checks if ECSTaskDefinitions specify a user for Amazon Elastic Container Service (Amazon ECS) EC2 launch type containers to run on. The rule is NON_COMPLIANT if the 'user' parameter is not present or set to 'root'.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_TASK_DEFINITION_NONROOT_USER

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-task-definition-pid-mode-check

Checks if ECSTaskDefinitions are configured to share a host's process namespace with its Amazon Elastic Container Service (Amazon ECS) containers. The rule is NON_COMPLIANT if the pidMode parameter is set to 'host'.

> **Note**
>
> This rule only evaluates the latest active revision of an Amazon ECS task definition.

**Identifier:** ECS_TASK_DEFINITION_PID_MODE_CHECK

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-task-definition-user-for-host-mode-check

Checks if Amazon ECS task definitions with host network mode have privileged OR nonroot in the container definition. The rule is NON_COMPLIANT if the latest active revision of a task definition has privileged=false (or is null) AND user=root (or is null).

> **Important**
>
> **Only one condition needs to be met for the rule to return compliant**
> The rule is COMPLIANT in any of following scenarios:
>
> - If the network mode is not set to host,
> - If the latest active revision of a task definition has privileged=true,
> - If the latest active revision of a task definition has a user that is not the root.
>
> This means that only one of these conditions need to be met for the rule to return compliant. To check specifically if a task definition has privileged=true, see ecs-containers-nonprivileged. To check specifically if a task definition has a user that is not the root, see ecs-task-definition-nonroot-user.

**Identifier:** ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

SkipInactiveTaskDefinitions (Optional), Type: boolean

Boolean flag to not check INACTIVE Amazon EC2 task definitions. If set to 'true', the rule won't evaluate INACTIVE Amazon EC2 task definitions. If set to 'false', the rule will evaluate the latest revision of INACTIVE Amazon EC2 task definitions.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ecs-task-definition-windows-user-non-admin

Checks if the latest active revision of an Amazon ECS task definition configures Windows containers to run as non-administrator users. The rule is NON_COMPLIANT if default administrator user is specified or user configuration is absent for any container.

**Identifier:** ECS_TASK_DEFINITION_WINDOWS_USER_NON_ADMIN

**Resource Types:** AWS::ECS::TaskDefinition

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-access-point-enforce-root-directory

Checks if Amazon Elastic File System (Amazon EFS) access points are configured to enforce a root directory. The rule is NON_COMPLIANT if the value of 'Path' is set to '/' (default root directory of the file system).

**Identifier:** EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

**Resource Types:** AWS::EFS::AccessPoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

approvedDirectories (Optional), Type: CSV

Comma-separated list of subdirectory paths that are approved for Amazon EFS access point root directory enforcement.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-access-point-enforce-user-identity

Checks if Amazon Elastic File System (Amazon EFS) access points are configured to enforce a user identity. The rule is NON_COMPLIANT if 'PosixUser' is not defined or if parameters are provided and there is no match in the corresponding parameter.

**Identifier:** EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

**Resource Types:** AWS::EFS::AccessPoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

approvedUids (Optional), Type: CSV

Comma-separated list of POSIX user ID that are approved for EFS access point user enforcement.

approvedGids (Optional), Type: CSV

Comma-separated list of POSIX group IDs that are approved for EFS access point user enforcement.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-automatic-backups-enabled

Checks if an Amazon Elastic File System (Amazon EFS) file system has automatic backups enabled. The rule is NON_COMPLIANT if `BackupPolicy.Status` is set to DISABLED.

**Identifier:** EFS_AUTOMATIC_BACKUPS_ENABLED

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-encrypted-check

Checks if Amazon Elastic File System (Amazon EFS) is configured to encrypt the file data using AWS Key Management Service (AWS KMS). The rule is NON_COMPLIANT if the encrypted key is set to false on `DescribeFileSystems` or if the `KmsKeyId` key on `DescribeFileSystems` does not match the `KmsKeyId` parameter.

**Identifier:** EFS_ENCRYPTED_CHECK

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

KmsKeyId (Optional), Type: String

Amazon Resource Name (ARN) of the KMS key that is used to encrypt the EFS file system.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-filesystem-ct-encrypted

Checks if Amazon Elastic File System (Amazon EFS) encrypts data with AWS Key Management Service (AWS KMS). The rule is NON_COMPLIANT if a file system is not encrypted. Optionally, you can check if a file system is not encrypted with specified KMS keys.

**Identifier:** EFS_FILESYSTEM_CT_ENCRYPTED

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

kmsKeyArns (Optional), Type: String

(Optional) Comma-separated list of Amazon Resource Names (ARNs) for AWS KMS keys. If provided, the rule checks if the specified KMS keys do not encrypt an Amazon EFS file system.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-file-system-tagged

Checks if Amazon Elastic File System file systems have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EFS_FILE_SYSTEM_TAGGED

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-in-backup-plan

Checks if Amazon Elastic File System (Amazon EFS) file systems are added in the backup plans of AWS Backup. The rule is NON_COMPLIANT if EFS file systems are not included in the backup plans.

**Identifier:** EFS_IN_BACKUP_PLAN

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon Elastic File System (Amazon EFS) File Systems. The rule is NON_COMPLIANT if the Amazon EFS File System does not have a corresponding Recovery Point created within the specified time period.

**Identifier:** EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon EFS File Systems for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of EFS File System for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-meets-restore-time-target

Checks if the restore time of Amazon Elastic File System (Amazon EFS) File Systems meets the specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of an Amazon EFS File System is greater than maxRestoreTime minutes.

**Identifier:** EFS_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags of Amazon EFS File Systems for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of EFS File System for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-mount-target-public-accessible

Checks if an Amazon Elastic File System (Amazon EFS) is associated with subnets that assign public IP addresses on launch. The rule is NON_COMPLIANT if the Amazon EFS mount target is associated with subnets that assign public IP addresses on launch.

**Identifier:** EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-resources-in-logically-air-gapped-vault

Checks if Amazon Elastic File System (Amazon EFS) File Systems are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon EFS File System is not in a logically air-gapped vault within the specified time period.

**Identifier:** EFS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon EFS File Systems for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of EFS File System for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 2184 for hours, 91 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## efs-resources-protected-by-backup-plan

Checks if Amazon Elastic File System (Amazon EFS) File Systems are protected by a backup plan. The rule is NON_COMPLIANT if the EFS File System is not covered by a backup plan.

**Identifier:** EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::EFS::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for EFS File Systems for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of the EFS File System for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eip-attached

Checks if all Elastic IP addresses that are allocated to an AWS account are attached to EC2 instances or in-use elastic network interfaces. The rule is NON_COMPLIANT if the 'AssociationId' is null for the Elastic IP address.

> **Note**
>
> Results might take up to 6 hours to become available after an evaluation occurs.

**Identifier:** EIP_ATTACHED

**Resource Types:** AWS::EC2::EIP

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

#### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-addon-tagged

Checks if Amazon EKS add-ons have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EKS_ADDON_TAGGED

**Resource Types:** AWS::EKS::Addon

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-cluster-logging-enabled

Checks if an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types.

**Identifier:** EKS_CLUSTER_LOGGING_ENABLED

**Resource Types:** AWS::EKS::Cluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-cluster-log-enabled

Checks if an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled or if logging is not enabled with the log type mentioned.

**Identifier:** EKS_CLUSTER_LOG_ENABLED

**Resource Types:** AWS::EKS::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

logTypes (Optional), Type: CSV

> Comma-separated list of EKS Cluster control plane log types for the rule to check. Valid values: "api", "audit", "authenticator", "controllerManager", "scheduler

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-cluster-oldest-supported-version

Checks if an Amazon Elastic Kubernetes Service (EKS) cluster is running the oldest supported version. The rule is NON_COMPLIANT if an EKS cluster is running oldest supported version (equal to the parameter '`oldestVersionSupported`').

**Identifier:** EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

**Resource Types:** AWS::EKS::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

oldestVersionSupported, Type: String

Value of the oldest version of Kubernetes supported on AWS.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-cluster-secrets-encrypted

Checks if Amazon EKS clusters are configured to have Kubernetes secrets encrypted using AWS KMS. The rule is NON_COMPLIANT if an EKS cluster does not have an encryptionConfig resource or if encryptionConfig does not name secrets as a resource.

**Identifier:** EKS_CLUSTER_SECRETS_ENCRYPTED

**Resource Types:** AWS::EKS::Cluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of KMS key Amazon Resource Names (ARNs) that are approved for EKS usage.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-cluster-supported-version

Checks if an Amazon Elastic Kubernetes Service (EKS) cluster is running a supported Kubernetes version. This rule is NON_COMPLIANT if an EKS cluster is running an unsupported version (less than the parameter '`oldestVersionSupported`').

**Identifier:** EKS_CLUSTER_SUPPORTED_VERSION

**Resource Types:** AWS::EKS::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

oldestVersionSupported, Type: String

Value of the oldest version of Kubernetes supported on AWS.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-endpoint-no-public-access

Checks if the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible.

**Identifier:** EKS_ENDPOINT_NO_PUBLIC_ACCESS

**Resource Types:** AWS::EKS::Cluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-fargate-profile-tagged

Checks if Amazon EKS fargate profiles have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EKS_FARGATE_PROFILE_TAGGED

**Resource Types:** AWS::EKS::FargateProfile

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## eks-secrets-encrypted

Checks if Amazon Elastic Kubernetes Service clusters are configured to have Kubernetes secrets encrypted using AWS Key Management Service (KMS) keys.

- This rule is COMPLIANT if an EKS cluster has an encryptionConfig with secrets as one of the resources.
- This rule is also COMPLIANT if the key used to encrypt EKS secrets matches with the parameter.
- This rule is NON_COMPLIANT if an EKS cluster does not have an encryptionConfig or if the encryptionConfig resources do not include secrets.
- This rule is also NON_COMPLIANT if the key used to encrypt EKS secrets does not match with the parameter.

**Identifier:** EKS_SECRETS_ENCRYPTED

**Resource Types:** AWS::EKS::Cluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma separated list of Amazon Resource Name (ARN) of the KMS key that should be used for encrypted secrets in an EKS cluster.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-automatic-backup-check-enabled

Checks if Amazon ElastiCache clusters (Valkey or Redis OSS) have automatic backup turned on. The rule is NON_COMPLIANT if automated backup is not enabled or the SnapshotRetentionLimit for a cluster is less than the specified `snapshotRetentionPeriod`.

**Identifier:** ELASTICACHE_AUTOMATIC_BACKUP_CHECK_ENABLED

**Resource Types:** AWS::ElastiCache::CacheCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

snapshotRetentionPeriod (Optional), Type: int

Minimum snapshot retention period in days for Valkey or Redis OSS. Valid values are 1 to 35. Default value is 1.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-auto-minor-version-upgrade-check

Checks if Amazon ElastiCache clusters have auto minor version upgrades enabled. The rule is NON_COMPLIANT for an ElastiCache cluster if it is using the Redis or Valkey engine and 'AutoMinorVersionUpgrade' is not set to 'true'.

**Identifier:** ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

**Resource Types:** AWS::ElastiCache::CacheCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-rbac-auth-enabled

Checks if Amazon ElastiCache replication groups have RBAC authentication enabled. The rule is NON_COMPLIANT if the Redis version is 6 or above and 'UserGroupIds' is missing, empty, or does not match an entry provided by the '`allowedUserGroupIDs`' parameter.

**Identifier:** ELASTICACHE_RBAC_AUTH_ENABLED

**Resource Types:** AWS::ElastiCache::ReplicationGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

allowedUserGroupIDs (Optional), Type: CSV

> A comma-separated list of User Group IDs that are approved for ElastiCache replication group access.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-redis-cluster-automatic-backup-check

Check if the Amazon ElastiCache Redis clusters have automatic backup turned on. The rule is NON_COMPLIANT if the SnapshotRetentionLimit for Redis cluster is less than the SnapshotRetentionPeriod parameter. For example: If the parameter is 15 then the rule is non-compliant if the snapshotRetentionPeriod is between 0-15.

**Identifier:** ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

**Resource Types:** AWS::ElastiCache::CacheCluster, AWS::ElastiCache::ReplicationGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

snapshotRetentionPeriod (Optional), Type: int, Default: 15

Minimum snapshot retention period in days for Redis cluster. Default is 15 days.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### elasticache-repl-grp-auto-failover-enabled

Checks if Amazon ElastiCache Redis replication groups have automatic failover enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if 'AutomaticFailover' is not set to 'enabled'.

**Identifier:** ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

**Resource Types:** AWS::ElastiCache::ReplicationGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-repl-grp-encrypted-at-rest

Checks if Amazon ElastiCache replication groups have encryption-at-rest enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if 'AtRestEncryptionEnabled' is disabled or if the KMS key ARN does not match the approvedKMSKeyArns parameter.

**Identifier:** ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

**Resource Types:** AWS::ElastiCache::ReplicationGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

approvedKMSKeyIds (Optional), Type: CSV

Comma-separated list of KMS Key IDs that are approved for ElastiCache usage.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-repl-grp-encrypted-in-transit

Checks if Amazon ElastiCache replication groups have encryption-in-transit enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if ‘TransitEncryptionEnabled’ is set to ‘false’.

**Identifier:** ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

**Resource Types:** AWS::ElastiCache::ReplicationGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-repl-grp-redis-auth-enabled

Checks if Amazon ElastiCache replication groups have Redis AUTH enabled. The rule is NON_COMPLIANT for an ElastiCache replication group if the Redis version of its nodes is below 6 (Version 6+ use Redis ACLs) and 'AuthToken' is missing or is empty/null.

**Identifier:** ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

**Resource Types:** AWS::ElastiCache::ReplicationGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-subnet-group-check

Checks if Amazon ElastiCache clusters are configured with a custom subnet group. The rule is NON_COMPLIANT for an ElastiCache cluster if it is using a default subnet group.

**Identifier:** ELASTICACHE_SUBNET_GROUP_CHECK

**Resource Types:** AWS::ElastiCache::CacheCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticache-supported-engine-version

Checks if ElastiCache clusters are running a version greater or equal to the recommended engine version. The rule is NON_COMPLIANT if the 'EngineVersion' for an ElastiCache cluster is less than the specified recommended version for its given engine.

**Identifier:** ELASTICACHE_SUPPORTED_ENGINE_VERSION

**Resource Types:** AWS::ElastiCache::CacheCluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

latestMemcachedVersion, Type: String

The latest recommended engine version for Memcached. Valid values are in semantic versioning (SemVer) format with 3-component number for major, minor, and patch versions (for example, 1.6.6, not 1.6).

latestRedisVersion, Type: String

The latest recommended engine version for Redis. Valid values are in semantic versioning (SemVer) format with 3-component number for major, minor, and patch versions (for example, 7.0.5, not 7.0).

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticbeanstalk-application-description

Checks if AWS Elastic Beanstalk applications have a description. The rule is NON_COMPLIANT if configuration.description does not exist or is an empty string.

**Identifier:** ELASTICBEANSTALK_APPLICATION_DESCRIPTION

**Resource Types:** AWS::ElasticBeanstalk::Application

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticbeanstalk-application-version-description

Checks if AWS Elastic Beanstalk application versions have a description. The rule is NON_COMPLIANT if configuration.description does not exist or is an empty string.

**Identifier:** ELASTICBEANSTALK_APPLICATION_VERSION_DESCRIPTION

**Resource Types:** AWS::ElasticBeanstalk::ApplicationVersion

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticbeanstalk-environment-description

Checks if AWS Elastic Beanstalk environments have a description. The rule is NON_COMPLIANT if configuration.description does not exist or is an empty string.

**Identifier:** ELASTICBEANSTALK_ENVIRONMENT_DESCRIPTION

**Resource Types:** AWS::ElasticBeanstalk::Environment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticsearch-encrypted-at-rest

Checks if Amazon OpenSearch Service (previously called Elasticsearch) domains have encryption at rest configuration enabled. The rule is NON_COMPLIANT if the EncryptionAtRestOptions field is not enabled.

**Identifier:** ELASTICSEARCH_ENCRYPTED_AT_REST

**Resource Types:** AWS::Elasticsearch::Domain

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticsearch-in-vpc-only

Checks if Amazon OpenSearch Service (previously called Elasticsearch) domains are in Amazon Virtual Private Cloud (Amazon VPC). The rule is NON_COMPLIANT if an OpenSearch Service domain endpoint is public.

**Identifier:** ELASTICSEARCH_IN_VPC_ONLY

**Resource Types:** AWS::Elasticsearch::Domain

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticsearch-logs-to-cloudwatch

Checks if OpenSearch Service (previously called Elasticsearch) domains are configured to send logs to CloudWatch Logs. The rule is COMPLIANT if a log is enabled for an OpenSearch Service domain. The rule is NON_COMPLIANT if logging is not configured.

**Identifier:** ELASTICSEARCH_LOGS_TO_CLOUDWATCH

**Resource Types:** AWS::Elasticsearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

logTypes (Optional), Type: CSV

Comma-separated list of logs that are enabled. Valid values are 'search', 'index', 'error'

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
```

```
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*An object with one or more of the following keys: `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS`, `AUDIT_LOGS`, depending on the types of logs you want to publish. Each key needs a valid `LogPublishingOption` value.

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elasticsearch-node-to-node-encryption-check

Check that Amazon OpenSearch Service nodes are encrypted end to end. The rule is NON_COMPLIANT if the node-to-node encryption is disabled on the domain.

**Identifier:** ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

**Resource Types:** AWS::Elasticsearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
```

```
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elastic-beanstalk-logs-to-cloudwatch

Checks if AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false.

**Identifier:** ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

**Resource Types:** AWS::ElasticBeanstalk::Environment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

RetentionInDays (Optional), Type: String

Checks the number of days to keep log events before they expire. Valid values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653. The rule is NON_COMPLIANT if the value of `logs.RetentionInDays` does not match this parameter.

DeleteOnTerminate (Optional), Type: String

Checks if logs are configured to be deleted upon termination of the environment. Valid values are `true` or `false`. The rule is NON_COMPLIANT if the value of `logs.DeleteOnTerminate` does not match this parameter.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elastic-beanstalk-managed-updates-enabled

Checks if managed platform updates in an AWS Elastic Beanstalk environment is enabled. The rule is COMPLIANT if the value for `ManagedActionsEnabled` is set to true. The rule is NON_COMPLIANT if the value for `ManagedActionsEnabled` is set to false, or if a parameter is provided and its value does not match the existing configurations.

**Identifier:** ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

**Resource Types:** AWS::ElasticBeanstalk::Environment

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Hyderabad), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Zurich) Region

**Parameters:**

UpdateLevel (Optional), Type: String

Indicates whether update levels are set to 'minor' version updates or a 'patch' version updates.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elbv2-acm-certificate-required

Checks if Application Load Balancers and Network Load Balancers have listeners that are configured to use certificates from AWS Certificate Manager (ACM). This rule is NON_COMPLIANT if at least 1 load balancer has at least 1 listener that is configured without a certificate from ACM or is configured with a certificate different from an ACM certificate.

**Identifier:** ELBV2_ACM_CERTIFICATE_REQUIRED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

AcmCertificatesAllowed (Optional), Type: CSV

Comma-separated list of certificate Amazon Resource Names (ARNs).

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elbv2-listener-encryption-in-transit

Checks if listeners for the load balancers are configured with HTTPS or TLS termination. The rule is NON_COMPLIANT if listeners are not configured with HTTPS or TLS termination.

**Identifier:** ELBV2_LISTENER_ENCRYPTION_IN_TRANSIT

**Resource Types:** AWS::ElasticLoadBalancingV2::Listener

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elbv2-multiple-az

Checks if an Elastic Load Balancer V2 (Application, Network, or Gateway Load Balancer) is mapped to multiple Availability Zones (AZs). The rule is NON_COMPLIANT if an Elastic Load Balancer V2 is mapped to less than 2 AZs. For more information, see Availability Zones for your Application Load Balancer.

**Identifier:** ELBV2_MULTIPLE_AZ

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

minAvailabilityZones (Optional), Type: int

Minimum number of expected AZs (between 2 and 10 inclusive).

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elbv2-predefined-security-policy-ssl-check

Checks if listeners for Application Load Balancers (ALBs) or Network Load Balancers (NLBs) use certain security policies. The rule is NON_COMPLIANT if an HTTPS listener for an ALB or a TLS listener for a NLB does not use the security policies you specify.

**Identifier:** ELBV2_PREDEFINED_SECURITY_POLICY_SSL_CHECK

**Resource Types:** AWS::ElasticLoadBalancingV2::Listener

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

sslPolicies, Type: CSV

Comma-separated list of SSL security policies for the rule to check. For example, "ELBSecurityPolicy-TLS13-1-2-2021-06".

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elb-acm-certificate-required

Checks if the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. This rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers.

**Identifier:** ELB_ACM_CERTIFICATE_REQUIRED

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Africa (Cape Town), Asia Pacific (Osaka), Europe (Milan), Israel (Tel Aviv), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elb-cross-zone-load-balancing-enabled

Checks if cross-zone load balancing is enabled for Classic Load Balancers. The rule is NON_COMPLIANT if cross-zone load balancing is not enabled for Classic Load Balancers.

**Identifier:** ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elb-custom-security-policy-ssl-check

Checks whether your Classic Load Balancer SSL listeners are using a custom policy. The rule is only applicable if there are SSL listeners for the Classic Load Balancer.

**Identifier:** ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

sslProtocolsAndCiphers, Type: CSV

Comma separated list of ciphers and protocols.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elb-deletion-protection-enabled

Checks whether an Elastic Load Balancer has deletion protection enabled. The rule is NON_COMPLIANT if deletion_protection.enabled is false.

**Identifier:** ELB_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elb-internal-scheme-check

Checks if a Classic Load Balancer scheme is internal. The rule is NON_COMPLIANT if configuration.scheme is not set to internal.

**Identifier:** ELB_INTERNAL_SCHEME_CHECK

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elb-logging-enabled

Checks if the Application Load Balancer and the Classic Load Balancer have logging enabled. The rule is NON_COMPLIANT if the `access_logs.s3.enabled` is false or `access_logs.S3.bucket` is not equal to the s3BucketName that you provided.

> **Note**
>
> The rule does not apply to Network Load Balancers or Gateway Load Balancers.

**Identifier:** ELB_LOGGING_ENABLED

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

s3BucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names for Amazon ELB to deliver the log files.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### elb-predefined-security-policy-ssl-check

Checks if your Classic Load Balancer SSL listeners use a predefined policy. The rule is NON_COMPLIANT if the Classic Load Balancer HTTPS/SSL listener's policy does not equal the value of the parameter '`predefinedPolicyName`'.

**Identifier:** ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

predefinedPolicyName, Type: String

Name of the predefined policy.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### elb-tagged

Checks if Classic Load Balancers have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ELB_TAGGED

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## elb-tls-https-listeners-only

Checks if your Classic Load Balancer is configured with SSL or HTTPS listeners. The rule is NON_COMPLIANT if a listener is not configured with SSL or HTTPS.

- If the Classic Load Balancer does not have a listener configured, then the rule returns `NOT_APPLICABLE`.
- The rule is COMPLIANT if the Classic Load Balancer listeners are configured with SSL or HTTPS.
- The rule is NON_COMPLIANT if a listener is not configured with SSL or HTTPS.

**Identifier:** ELB_TLS_HTTPS_LISTENERS_ONLY

**Resource Types:** AWS::ElasticLoadBalancing::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## emr-block-public-access

Checks if an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges.

**Identifier:** EMR_BLOCK_PUBLIC_ACCESS

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## emr-kerberos-enabled

Checks if Amazon EMR clusters have Kerberos enabled. The rule is NON_COMPLIANT if a security configuration is not attached to the cluster or the security configuration does not satisfy the specified rule parameters.

**Identifier:** EMR_KERBEROS_ENABLED

**Resource Types:** AWS::EMR::Cluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

TicketLifetimeInHours (Optional), Type: int

Period for which Kerberos ticket issued by cluster's KDC is valid.

Realm (Optional), Type: String

Kereberos realm name of the other realm in the trust relationship.

Domain (Optional), Type: String

Domain name of the other realm in the trust relationship.

AdminServer (Optional), Type: String

Fully qualified domain of the admin server in the other realm of the trust relationship.

KdcServer (Optional), Type: String

Fully qualified domain of the KDC server in the other realm of the trust relationship.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### emr-master-no-public-ip

Checks if Amazon EMR clusters' master nodes have public IPs. The rule is NON_COMPLIANT if the master node has a public IP.

> **Note**
>
> This rule checks clusters that are in RUNNING or WAITING state. This rule requires you to enable recording for the `AWS::EC2::Instance` resource type in order to have an accurate evaluation.

**Identifier:** EMR_MASTER_NO_PUBLIC_IP

**Resource Types:** AWS::EMR::Cluster, AWS::EC2::Instance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## emr-security-configuration-encryption-rest

Checks if an Amazon EMR security configuration has encryption at rest enabled. The rule is NON_COMPLIANT if configuration.SecurityConfiguration.EncryptionConfiguration.EnableAtRestEncryption is false.

**Identifier:** EMR_SECURITY_CONFIGURATION_ENCRYPTION_REST

**Resource Types:** AWS::EMR::SecurityConfiguration

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## emr-security-configuration-encryption-transit

Checks if an Amazon EMR security configuration has encryption in transit enabled. The rule is NON_COMPLIANT if configuration.SecurityConfiguration.EncryptionConfiguration.EnableInTransitEncryption is false.

**Identifier:** EMR_SECURITY_CONFIGURATION_ENCRYPTION_TRANSIT

**Resource Types:** AWS::EMR::SecurityConfiguration

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## encrypted-volumes

Checks if attached Amazon EBS volumes are encrypted and optionally are encrypted with a specified KMS key. The rule is NON_COMPLIANT if attached EBS volumes are unencrypted or are encrypted with a KMS key not in the supplied parameters.

**Identifier:** ENCRYPTED_VOLUMES

**Resource Types:** AWS::EC2::Volume

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

kmsId (Optional), Type: String

ID or ARN of the KMS key that is used to encrypt the volume.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## event-data-store-cmk-encryption-enabled

Checks if AWS Cloud Trail event data stores have customer managed AWS KMS keys enabled. The rule is NON_COMPLIANT if an event data store has disabled customer managed KMS keys. Optionally, you can specify a list of KMS keys for the rule to check.

**Identifier:** EVENT_DATA_STORE_CMK_ENCRYPTION_ENABLED

**Resource Types:** AWS::CloudTrail::EventDataStore

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of Amazon Resource Names (ARNs) of AWS KMS keys for the rule to check. If provided, the rule is NON_COMPLIANT if an AWS Cloud Trail event data store is not encrypted with one of these KMS keys.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## evidently-launch-description

Checks if Amazon CloudWatch Evidently launches have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** EVIDENTLY_LAUNCH_DESCRIPTION

**Resource Types:** AWS::Evidently::Launch

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## evidently-launch-tagged

Checks if Amazon CloudWatch Evidently launches have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EVIDENTLY_LAUNCH_TAGGED

**Resource Types:** AWS::Evidently::Launch

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### evidently-project-description

Checks if Amazon CloudWatch Evidently projects have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** EVIDENTLY_PROJECT_DESCRIPTION

**Resource Types:** AWS::Evidently::Project

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### evidently-project-tagged

Checks if Amazon CloudWatch Evidently projects have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EVIDENTLY_PROJECT_TAGGED

**Resource Types:** AWS::Evidently::Project

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## evidently-segment-description

Checks if Amazon CloudWatch Evidently segments have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** EVIDENTLY_SEGMENT_DESCRIPTION

**Resource Types:** AWS::Evidently::Segment

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## evidently-segment-tagged

Checks if Amazon CloudWatch Evidently segments have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** EVIDENTLY_SEGMENT_TAGGED

**Resource Types:** AWS::Evidently::Segment

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fis-experiment-template-log-configuration-exists

Checks if AWS FIS experiment templates have experiment logging configured. The rule is NON_COMPLIANT if configuration.LogConfiguration does not exist.

**Identifier:** FIS_EXPERIMENT_TEMPLATE_LOG_CONFIGURATION_EXISTS

**Resource Types:** AWS::FIS::ExperimentTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fis-experiment-template-tagged

Checks if AWS FIS experiment templates have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** FIS_EXPERIMENT_TEMPLATE_TAGGED

**Resource Types:** AWS::FIS::ExperimentTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fms-shield-resource-policy-check

> **Note**
>
> This rule is currently in the deprecation process. We do not recommend that you use them directly.

Checks if resources that AWS Shield Advanced can protect are protected by Shield Advanced. The rule is NON_COMPLIANT if a specified resource is not protected.

**Identifier:** FMS_SHIELD_RESOURCE_POLICY_CHECK

**Resource Types:** AWS::CloudFront::Distribution, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ShieldRegional::Protection, AWS::Shield::Protection

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

webACLId, Type: String

A unique identifier for a Web ACL.

resourceTypes, Type: String

The resource types you specify for the rule to check.

resourceTags (Optional), Type: String

The resource tags you specify for the rule to check. For example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }.

excludeResourceTags (Optional), Type: boolean

If true, the rule excludes the resources specified in resourceTags. If false, the rule includes all the resources specified in resourceTags.

fmsManagedToken (Optional), Type: String

A token generated by AWS Firewall Manager when creating the rule in your account. AWS Config ignores this parameter when you create this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, AWS Firewall Manager will update NON_COMPLIANT resources according to FMS policy. AWS Config ignores this parameter when you create this rule.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fms-webacl-resource-policy-check

> **Note**
>
> This rule is currently in the deprecation process. We do not recommend that you use them directly.

Checks if the web ACL is associated with an Application Load Balancer, API Gateway stage, or Amazon CloudFront distributions. When AWS Firewall Manager creates this rule, the FMS policy owner specifies the `WebACLId` in the FMS policy and can optionally enable remediation.

**Identifier:** FMS_WEBACL_RESOURCE_POLICY_CHECK

**Resource Types:** AWS::CloudFront::Distribution, AWS::ApiGateway::Stage, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

webACLId, Type: String

The WebACLId of the web ACL.

resourceTags (Optional), Type: String

The resource tags (ApplicationLoadBalancer, ApiGatewayStage and CloudFront distributions) that the rule should be associated with. (for example, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] })

excludeResourceTags (Optional), Type: boolean

If true, exclude resources that match resourceTags.

fmsManagedToken (Optional), Type: String

A token generated by AWS Firewall Manager when creating the rule in customer account. AWS Config ignores this parameter when customer creates this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, AWS Firewall Manager will update non-compliant resources according to FMS policy. AWS Config ignores this parameter when customer creates this rule.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fms-webacl-rulegroup-association-check

> **Note**
>
> This rule is currently in the deprecation process. We do not recommend that you use them directly.

Checks if the rule groups associate with the web ACL at the correct priority. The correct priority is decided by the rank of the rule groups in the ruleGroups parameter. When AWS Firewall Manager creates this rule, it assigns the highest priority 0 followed by 1, 2, and so on. The FMS policy owner specifies the `ruleGroups` rank in the FMS policy and can optionally enable remediation.

**Identifier:** FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

**Resource Types:** AWS::WAF::WebACL, AWS::WAFRegional::WebACL

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

ruleGroups, Type: String

Comma-separated list of RuleGroupIds and WafOverrideAction pairs. (for example, ruleGroupId-1:NONE, ruleGroupId2:COUNT)

fmsManagedToken (Optional), Type: String

A token generated by AWS Firewall Manager when creating the rule in customer account. AWS Config ignores this parameter when customer creates this rule.

fmsRemediationEnabled (Optional), Type: boolean

If true, AWS Firewall Manager will update non-compliant resources according to FMS policy. AWS Config ignores this parameter when customer creates this rule.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## frauddetector-entity-type-tagged

Checks if Amazon Fraud Detector entity types have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** FRAUDDETECTOR_ENTITY_TYPE_TAGGED

**Resource Types:** AWS::FraudDetector::EntityType

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (Ohio), Europe (Ireland), US East (N. Virginia), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## frauddetector-label-tagged

Checks if Amazon Fraud Detector labels have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** FRAUDDETECTOR_LABEL_TAGGED

**Resource Types:** AWS::FraudDetector::Label

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (Ohio), Europe (Ireland), US East (N. Virginia), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## frauddetector-outcome-tagged

Checks if Amazon Fraud Detector outcomes have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** FRAUDDETECTOR_OUTCOME_TAGGED

**Resource Types:** AWS::FraudDetector::Outcome

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (Ohio), Europe (Ireland), US East (N. Virginia), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## frauddetector-variable-tagged

Checks if Amazon Fraud Detector variables have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** FRAUDDETECTOR_VARIABLE_TAGGED

**Resource Types:** AWS::FraudDetector::Variable

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (Ohio), Europe (Ireland), US East (N. Virginia), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon FSx File Systems. The rule is NON_COMPLIANT if the Amazon FSx File System does not have a corresponding recovery point created within the specified time period.

**Identifier:** FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon FSx File Systems for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Amazon FSx File System for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-lustre-copy-tags-to-backups

Checks if the Amazon FSx for Lustre file systems are configured to copy tags to backups. The rule is NON_COMPLIANT if Lustre file systems are not configured to copy tags to backups.

**Identifier:** FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-meets-restore-time-target

Checks if the restore time of Amazon FSx File Systems meets the specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of an Amazon FSx File System is greater than maxRestoreTime minutes.

**Identifier:** FSX_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags of Amazon FSx File Systems for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Amazon FSx File System for the rule to check.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-ontap-deployment-type-check

Checks if Amazon FSx for NetApp ONTAP file systems are configured with certain deployment types. The rule is NON_COMPLIANT if the Amazon FSx for NetApp ONTAP file systems are not configured with the deployment types you specify.

**Identifier:** FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

deploymentTypes, Type: CSV

Comma-separated list of allowed Deployment types for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-openzfs-copy-tags-enabled

Checks if the Amazon FSx for OpenZFS file systems are configured to copy tags to backups and volumes. The rule is NON_COMPLIANT if FSx for OpenZFS file systems are not configured to copy tags to backups and volumes.

**Identifier:** FSX_OPENZFS_COPY_TAGS_ENABLED

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-openzfs-deployment-type-check

Checks if the Amazon FSx for OpenZFS file systems are configured with certain deployment types. The rule is NON_COMPLIANT if FSx for OpenZFS file systems are not configured with the deployment types you specify.

**Identifier:** FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

deploymentTypes, Type: CSV

Comma-separated list of allowed Deployment types for the rule to check.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-resources-protected-by-backup-plan

Checks if Amazon FSx File Systems are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon FSx File System is not covered by a backup plan.

**Identifier:** FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon FSx File Systems for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of the Amazon FSx File System for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-windows-audit-log-configured

Checks if the Amazon FSx for Windows File Server file systems have file access auditing enabled. The rule is NON_COMPLIANT if the FSx for Windows File Server file systems do not have file access auditing enabled.

**Identifier:** FSX_WINDOWS_AUDIT_LOG_CONFIGURED

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## fsx-windows-deployment-type-check

Checks if the Amazon FSx for WINDOWS file systems are configured with certain deployment types. The rule is NON_COMPLIANT if FSx for WINDOWS file systems are not configured with the deployment types you specify.

**Identifier:** FSX_WINDOWS_DEPLOYMENT_TYPE_CHECK

**Resource Types:** AWS::FSx::FileSystem

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Europe (Paris), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

deploymentTypes, Type: CSV

Comma-separated list of allowed Deployment types for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## glb-listener-tagged

Checks if Gateway Load Balancer listeners have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** GLB_LISTENER_TAGGED

**Resource Types:** AWS::ElasticLoadBalancingV2::Listener

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## glb-tagged

Checks if Gateway Load Balancers have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** GLB_TAGGED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## global-endpoint-event-replication-enabled

Checks if event replication is enabled for Amazon EventBridge global endpoints. The rule is NON_COMPLIANT if event replication is not enabled.

**Identifier:** GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

**Resource Types:** AWS::Events::Endpoint

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Osaka), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## glue-job-logging-enabled

Checks if an AWS Glue job has logging enabled. The rule is NON_COMPLIANT if an AWS Glue job does not have Amazon CloudWatch logs enabled.

**Identifier:** GLUE_JOB_LOGGING_ENABLED

**Resource Types:** AWS::Glue::Job

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## glue-ml-transform-encrypted-at-rest

Checks if an AWS Glue ML Transform has encryption at rest enabled. The rule is NON_COMPLIANT if `MLUserDataEncryptionMode` is set to `DISABLED`.

**Identifier:** GLUE_ML_TRANSFORM_ENCRYPTED_AT_REST

**Resource Types:** AWS::Glue::MLTransform

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## glue-ml-transform-tagged

Checks if AWS Glue machine learning transforms have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** GLUE_ML_TRANSFORM_TAGGED

**Resource Types:** AWS::Glue::MLTransform

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## glue-spark-job-supported-version

Checks if an AWS Glue Spark job is running on the specified minimum supported AWS Glue version. The rule is NON_COMPLIANT if the AWS Glue Spark job is not running on the minimum supported AWS Glue version that you specify.

**Identifier:** GLUE_SPARK_JOB_SUPPORTED_VERSION

**Resource Types:** AWS::Glue::Job

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

minimumSupportedGlueVersion, Type: String

String value you must specify of the minimum supported AWS Glue version for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-ec2-protection-runtime-enabled

Checks if ECS Runtime Monitoring with automated agent management is enabled for Amazon GuardDuty detector. The rule is NON_COMPLIANT if the feature is not enabled for your account or at least one member account in your organization.

**Identifier:** GUARDDUTY_EC2_PROTECTION_RUNTIME_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-ecs-protection-runtime-enabled

Checks if ECS Runtime Monitoring with automated agent management is enabled for Amazon GuardDuty detector. The rule is NON_COMPLIANT if the feature is not enabled for your account or at least one member account in your organization.

**Identifier:** GUARDDUTY_ECS_PROTECTION_RUNTIME_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-eks-protection-audit-enabled

Checks if Audit Log Monitoring for Amazon Elastic Kubernetes Service (Amazon EKS) is enabled for an Amazon GuardDuty detector in your account. The rule is NON_COMPLIANT if the EKS Audit Log Monitoring feature is not enabled for your account.

**Identifier:** GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-eks-protection-runtime-enabled

Checks if Amazon EKS Runtime Monitoring with automated agent management is enabled for GuardDuty detector in your account. The rule is NON_COMPLIANT if EKS Runtime Monitoring with automated agent management in GuardDuty is not enabled for your account.

**Identifier:** GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-enabled-centralized

Checks if Amazon GuardDuty is enabled in your AWS account and AWS Region. If you provide an AWS account for centralization, the rule evaluates the GuardDuty results in the centralized account. The rule is COMPLIANT when GuardDuty is enabled.

**Identifier:** GUARDDUTY_ENABLED_CENTRALIZED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

CentralMonitoringAccount (Optional), Type: String

Comma separated list of AWS Accounts (12-digit) where Amazon GuardDuty results are allowed to be centralized.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-lambda-protection-enabled

Checks if Lambda Protection is enabled for an Amazon GuardDuty detector in your account. The rule is NON_COMPLIANT if the Lambda Protection feature in Amazon GuardDuty is not enabled for your account.

**Identifier:** GUARDDUTY_LAMBDA_PROTECTION_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-malware-protection-enabled

Checks if Malware Protection is enabled for an Amazon GuardDuty detector in your account. The rule is NON_COMPLIANT if the Malware Protection feature in Amazon GuardDuty is not enabled for your account.

**Identifier:** GUARDDUTY_MALWARE_PROTECTION_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-non-archived-findings

Checks if Amazon GuardDuty has findings that are non-archived. The rule is NON_COMPLIANT if GuardDuty has non-archived low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev/`daysHighSev` parameter.

**Identifier:** GUARDDUTY_NON_ARCHIVED_FINDINGS

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

daysLowSev (Optional), Type: int, Default: 30

The number of days Amazon GuardDuty low severity findings are allowed to stay non archived. The default is 30 days.

daysMediumSev (Optional), Type: int, Default: 7

The number of days Amazon GuardDuty medium severity findings are allowed to stay non archived. The default is 7 days.

daysHighSev (Optional), Type: int, Default: 1

The number of days Amazon GuardDuty high severity findings are allowed to stay non archived. The default is 1 day.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-rds-protection-enabled

Checks if Amazon Relational Database Service (Amazon RDS) protection is enabled for an Amazon GuardDuty detector in your account. The rule is NON_COMPLIANT if the Amazon RDS protection feature in Amazon GuardDuty is not enabled for you account.

**Identifier:** GUARDDUTY_RDS_PROTECTION_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-runtime-monitoring-enabled

Checks if Runtime Monitoring is enabled for Amazon GuardDuty detector in your account or organization. The rule is NON_COMPLIANT if Runtime Monitoring in GuardDuty is not enabled for your account or at least one member account in your organization.

**Identifier:** GUARDDUTY_RUNTIME_MONITORING_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## guardduty-s3-protection-enabled

Checks if S3 Protection is enabled for an Amazon GuardDuty Detector in your account. The rule is NON_COMPLIANT if the S3 Protection feature in Amazon GuardDuty is not enabled for your account.

**Identifier:** GUARDDUTY_S3_PROTECTION_ENABLED

**Resource Types:** AWS::GuardDuty::Detector

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-customer-policy-blocked-kms-actions

Checks if the managed AWS Identity and Access Management (IAM) policies that you create do not allow blocked KMS actions on all AWS KMS key resources. The rule is NON_COMPLIANT if any blocked action is allowed on all AWS KMS keys by the managed IAM policy.

> **Note**
>
> To be considered non-public, an IAM policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

**Identifier:** IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

**Resource Types:** AWS::IAM::Policy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

blockedActionsPatterns, Type: CSV

Comma-separated list of blocked KMS action patterns for the rule to check. The rule is NON_COMPLIANT if IAM customer managed policies allow wildcard access to all resources for the actions you specify.

excludePermissionBoundaryPolicy (Optional), Type: boolean

Boolean flag to exclude the evaluation of IAM policies used as permissions boundaries. If set to 'true', the rule will not include permissions boundaries in the evaluation. Otherwise, all IAM policies in scope are evaluated when value is set to 'false.' Default value is 'false'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-external-access-analyzer-enabled

Checks if an IAM Access Analyzer for external access is activated in your account per region. The rule is NON_COMPLIANT if there are no analyzers for external access in the region or if the 'status' attribute is not set to 'ACTIVE'.

**Identifier:** IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-group-has-users-check

Checks whether IAM groups have at least one IAM user.

**Identifier:** IAM_GROUP_HAS_USERS_CHECK

**Resource Types:** AWS::IAM::Group

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-inline-policy-blocked-kms-actions

Checks if the inline policies attached to your IAM users, roles, and groups do not allow blocked actions on all AWS KMS keys. The rule is NON_COMPLIANT if any blocked action is allowed on all AWS KMS keys in an inline policy.

**Identifier:** IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

**Resource Types:** AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

blockedActionsPatterns, Type: CSV

Comma-separated list of blocked KMS action patterns, for example, kms:*, kms:Decrypt, kms:ReEncrypt*.

excludeRoleByManagementAccount (Optional), Type: boolean

Exclude a role if it is only assumable by organization management account.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-no-inline-policy-check

Checks if the inline policy feature is not in use. The rule is NON_COMPLIANT if an AWS Identity and Access Management (IAM) user, IAM role or IAM group has any inline policy.

**Identifier:** IAM_NO_INLINE_POLICY_CHECK

**Resource Types:** AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), US West (N. California), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-oidc-provider-tagged

Checks if AWS IAM OIDC providers have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IAM_OIDC_PROVIDER_TAGGED

**Resource Types:** AWS::IAM::OIDCProvider

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-password-policy

Checks if the account password policy for AWS Identity and Access Management (IAM) users meets the specified requirements indicated in the parameters. The rule is NON_COMPLIANT if the account password policy does not meet the specified requirements.

**Important**

The `true` and `false` values for the rule parameters are case-sensitive. If `true` is not provided in lowercase, it will be treated as `false`.

**Note**

**Evaluation Result for the Default IAM Password Policy**
This rule is marked as NON_COMPLIANT when the default IAM password policy is used.
**Managed Rules and Global IAM Resource Types**
The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** IAM_PASSWORD_POLICY

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

RequireUppercaseCharacters (Optional), Type: boolean, Default: true

Require at least one uppercase character in password.

RequireLowercaseCharacters (Optional), Type: boolean, Default: true

Require at least one lowercase character in password.

RequireSymbols (Optional), Type: boolean, Default: true

Require at least one symbol in password.

RequireNumbers (Optional), Type: boolean, Default: true

Require at least one number in password.

MinimumPasswordLength (Optional), Type: int, Default: 14

Password minimum length.

PasswordReusePrevention (Optional), Type: int, Default: 24

Number of passwords before allowing reuse.

MaxPasswordAge (Optional), Type: int, Default: 90

Number of days before password expiration.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-policy-blacklisted-check

Checks in each AWS Identity and Access Management (IAM) resource, if a policy Amazon Resource Name (ARN) in the input parameter is attached to the IAM resource. The rule is NON_COMPLIANT if the policy ARN is attached to the IAM resource.

**Identifier:** IAM_POLICY_BLACKLISTED_CHECK

**Resource Types:** AWS::IAM::User, AWS::IAM::Group, AWS::IAM::Role

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

policyArns, Type: CSV, Default: arn:aws:iam::aws:policy/AdministratorAccess

Comma separated list of IAM policy arns which should not be attached to any IAM entity.

exceptionList (Optional), Type: CSV

Comma separated list of resourcetypes and list of resource name pairs. For example, users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3].

> **Note**
>
> For the exception list, specify the name of the resource and not the full ARN. Not valid: `arn:aws:iam::444455556666:role/Admin`. Valid: `Admin`.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-policy-in-use

Checks whether the IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity.

> **Note**
>
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of

which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** IAM_POLICY_IN_USE

**Resource Types:** AWS::IAM::Policy

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

policyARN, Type: String

An IAM policy ARN to be checked.

policyUsageType (Optional), Type: String

Specify whether you expect the policy to be attached to an IAM user, group or role. Valid values are IAM_USER, IAM_GROUP, IAM_ROLE, or ANY. Default value is ANY.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-policy-no-statements-with-admin-access

Checks if AWS Identity and Access Management (IAM) policies that you create have Allow statements that grant permissions to all actions on all resources. The rule is NON_COMPLIANT if any customer managed IAM policy statement includes "Effect": "Allow" with "Action": "*" over "Resource": "*".

> **Note**
>
> This rule only evaluates customer managed policies. This rule does NOT evaluate inline policies or AWS managed policies. For more information on the difference, see Managed policies and inline policies in the *IAM User Guide*.

The following policy is NON_COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

The following policy is COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

**Identifier:** IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

**Resource Types:** AWS::IAM::Policy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

excludePermissionBoundaryPolicy (Optional), Type: boolean

Boolean flag to exclude the evaluation of IAM policies used as permissions boundaries. If set to 'true', the rule will not include permissions boundaries in the evaluation. Otherwise, all IAM policies in scope are evaluated when value is set to 'false.' Default value is 'false'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-policy-no-statements-with-full-access

Checks if AWS Identity and Access Management (IAM) policies that you create grant permissions to all actions on individual AWS resources. The rule is NON_COMPLIANT if any customer managed IAM policy allows full access to at least 1 AWS service.

**Context**: Following the principle of least privilege, it is recommended to limit the permitted actions in your IAM policies when granting permissions to AWS services. This approach helps ensure that you only grant the necessary permissions by specifying the exact actions required, avoiding the use of unrestricted wildcards for a service, such as `ec2:*`.

In some cases, you might want to permit multiple actions with a similar prefix, such as DescribeFlowLogs and DescribeAvailabilityZones. In these cases, you can add a suffixed wildcard to the common prefix (for example, `ec2:Describe*`). Grouping related actions can help avoid hitting IAM policy size limits.

This rule will return COMPLIANT if you use prefixed actions with a suffixed wildcard (for example, `ec2:Describe*`). This rule will only return NON_COMPLIANT if you use unrestricted wildcards (for example, `ec2:*`).

> **Note**
>
> This rule only evaluates customer managed policies. This rule does NOT evaluate inline policies or AWS managed policies. For more information on the difference, see Managed policies and inline policies in the *IAM User Guide*.

**Identifier:** IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

**Resource Types:** AWS::IAM::Policy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

excludePermissionBoundaryPolicy (Optional), Type: boolean

> Boolean flag to exclude the evaluation of IAM policies used as permissions boundaries. If set to 'true', the rule will not include permissions boundaries in the evaluation. Otherwise, all IAM policies in scope are evaluated when value is set to 'false.' Default value is 'false'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-role-managed-policy-check

Checks if all managed policies specified in the list of managed policies are attached to the AWS Identity and Access Management (IAM) role. The rule is NON_COMPLIANT if a managed policy is not attached to the IAM role.

**Identifier:** IAM_ROLE_MANAGED_POLICY_CHECK

**Resource Types:** AWS::IAM::Role

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

managedPolicyArns, Type: CSV

Comma-separated list of AWS managed policy Amazon Resource Names (ARNs). For more information, see Amazon Resource Names (ARNs) and AWS managed policies in the *IAM User Guide*.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-root-access-key-check

Checks if the root user access key is available. The rule is COMPLIANT if the user access key does not exist. Otherwise, NON_COMPLIANT.

> **Note**
>
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** IAM_ROOT_ACCESS_KEY_CHECK

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-saml-provider-tagged

Checks if AWS IAM SAML providers have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IAM_SAML_PROVIDER_TAGGED

**Resource Types:** AWS::IAM::SAMLProvider

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-server-certificate-expiration-check

Checks if AWS IAM SSL/TLS server certificates stored in IAM are expired. The rule is NON_COMPLIANT if an IAM server certificate is expired.

**Identifier:** IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

**Resource Types:** AWS::IAM::ServerCertificate

**Trigger type:** Periodic

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-server-certificate-tagged

Checks if AWS IAM server certificates have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IAM_SERVER_CERTIFICATE_TAGGED

**Resource Types:** AWS::IAM::ServerCertificate

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-user-group-membership-check

Checks whether IAM users are members of at least one IAM group.

**Identifier:** IAM_USER_GROUP_MEMBERSHIP_CHECK

**Resource Types:** AWS::IAM::User

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

groupNames (Optional), Type: CSV

Comma-separated list of IAM groups in which IAM users must be members.

> **Note**
>
> This rule does not support group names with commas.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iam-user-mfa-enabled

Checks if the AWS Identity and Access Management (IAM) users have multi-factor authentication (MFA) enabled. The rule is NON_COMPLIANT if MFA is not enabled for at least one IAM user.

> **Note**
>
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** IAM_USER_MFA_ENABLED

**Resource Types:** AWS::IAM::User

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### iam-user-no-policies-check

Checks if none of your AWS Identity and Access Management (IAM) users have policies attached. IAM users must inherit permissions from IAM groups or roles. The rule is NON_COMPLIANT if there is at least one policy that is attached to the IAM user.

**Identifier:** IAM_USER_NO_POLICIES_CHECK

**Resource Types:** AWS::IAM::User

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### iam-user-unused-credentials-check

Checks if your AWS Identity and Access Management (IAM) users have passwords or active access keys that have not been used within the specified number of days you provided. The rule is NON_COMPLIANT if there are inactive accounts not recently used.

> **Note**
>
> **Re-evaluation Timeline**
> Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.
> **Managed Rules and Global IAM Resource Types**

The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** IAM_USER_UNUSED_CREDENTIALS_CHECK

**Resource Types:** AWS::IAM::User

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

maxCredentialUsageAge, Type: int, Default: 90

Maximum number of days a credential cannot be used. The default value is 90 days.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## restricted-ssh

> **Important**
>
> For this rule, the rule identifier (INCOMING_SSH_DISABLED) and rule name (restricted-ssh) are different.

Checks if the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT.

**Identifier:** INCOMING_SSH_DISABLED

**Resource Types:** AWS::EC2::SecurityGroup

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## inspector-ec2-scan-enabled

Checks if Amazon Inspector V2 EC2 scanning is activated for your single or multi-account environment to detect potential vulnerabilities and network reachability issues on your EC2 instances. The rule is NON_COMPLIANT if EC2 scanning is not activated.

**Identifier:** INSPECTOR_EC2_SCAN_ENABLED

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## inspector-ecr-scan-enabled

Checks if Amazon Inspector V2 ECR scanning is activated for your single or multi-account environment to detect potential software vulnerabilities in your container images. The rule is NON_COMPLIANT if ECR scanning is not activated.

**Identifier:** INSPECTOR_ECR_SCAN_ENABLED

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## inspector-lambda-code-scan-enabled

Checks if Amazon Inspector V2 Lambda code scanning is activated for your single or multi-account environment to detect potential code vulnerabilities. The rule is NON_COMPLIANT if Lambda code scanning is not activated.

**Identifier:** INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** Only available in Europe (Stockholm), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## inspector-lambda-standard-scan-enabled

Checks if Amazon Inspector V2 Lambda standard scanning is activated for your single or multi-account environment to detect potential software vulnerabilities. The rule is NON_COMPLIANT if Lambda standard scanning is not activated.

**Identifier:** INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### ec2-instances-in-vpc

> **Important**
>
> For this rule, the rule identifier (INSTANCES_IN_VPC) and rule name (ec2-instances-in-vpc) are different.

Checks if your EC2 instances belong to a virtual private cloud (VPC). Optionally, you can specify the VPC ID to associate with your instances.

**Identifier:** INSTANCES_IN_VPC

**Resource Types:** AWS::EC2::Instance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

vpcId (Optional), Type: String

VPC ID that contains these EC2 instances.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### internet-gateway-authorized-vpc-only

Checks if internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC.

**Identifier:** INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

**Resource Types:** AWS::EC2::InternetGateway

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

AuthorizedVpcIds (Optional), Type: CSV

Comma-separated list of the authorized VPC IDs with attached IGWs. If parameter is not provided all attached IGWs will be NON_COMPLIANT.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotdevicedefender-custom-metric-tagged

AWS IoT Device Defender custom metrics have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTDEVICEDEFENDER_CUSTOM_METRIC_TAGGED

**Resource Types:** AWS::IoT::CustomMetric

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Middle East (Bahrain), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Middle East (UAE), Europe (Frankfurt), Asia Pacific (Hong Kong), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotevents-alarm-model-tagged

Checks if AWS IoT Events alarm models have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTEVENTS_ALARM_MODEL_TAGGED

**Resource Types:** AWS::IoTEvents::AlarmModel

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotevents-detector-model-tagged

Checks if AWS IoT Events detector models have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTEVENTS_DETECTOR_MODEL_TAGGED

**Resource Types:** AWS::IoTEvents::DetectorModel

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotevents-input-tagged

Checks if AWS IoT Events inputs have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTEVENTS_INPUT_TAGGED

**Resource Types:** AWS::IoTEvents::Input

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotsitewise-asset-model-tagged

Checks if AWS IoT SiteWise asset models have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTSITEWISE_ASSET_MODEL_TAGGED

**Resource Types:** AWS::IoTSiteWise::AssetModel

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotsitewise-dashboard-tagged

Checks if AWS IoT SiteWise dashboards have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTSITEWISE_DASHBOARD_TAGGED

**Resource Types:** AWS::IoTSiteWise::Dashboard

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotsitewise-gateway-tagged

Checks if AWS IoT SiteWise gateways have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTSITEWISE_GATEWAY_TAGGED

**Resource Types:** AWS::IoTSiteWise::Gateway

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotsitewise-portal-tagged

Checks if AWS IoT SiteWise portals have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTSITEWISE_PORTAL_TAGGED

**Resource Types:** AWS::IoTSiteWise::Portal

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotsitewise-project-tagged

Checks if AWS IoT SiteWise projects have tags. Optionally, you can specify tag keys for the rule. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTSITEWISE_PROJECT_TAGGED

**Resource Types:** AWS::IoTSiteWise::Project

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iottwinmaker-component-type-tagged

Checks if AWS IoT TwinMaker component types have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTTWINMAKER_COMPONENT_TYPE_TAGGED

**Resource Types:** AWS::IoTTwinMaker::ComponentType

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iottwinmaker-entity-tagged

Checks if AWS IoT TwinMaker entities have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTTWINMAKER_ENTITY_TAGGED

**Resource Types:** AWS::IoTTwinMaker::Entity

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iottwinmaker-scene-tagged

Checks if AWS IoT TwinMaker scenes have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTTWINMAKER_SCENE_TAGGED

**Resource Types:** AWS::IoTTwinMaker::Scene

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iottwinmaker-sync-job-tagged

Checks if AWS IoT TwinMaker sync jobs have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTTWINMAKER_SYNC_JOB_TAGGED

**Resource Types:** AWS::IoTTwinMaker::SyncJob

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iottwinmaker-workspace-tagged

Checks if AWS IoT TwinMaker workspaces have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTTWINMAKER_WORKSPACE_TAGGED

**Resource Types:** AWS::IoTTwinMaker::Workspace

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotwireless-fuota-task-tagged

Checks if AWS IoT Wireless FUOTA tasks have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTWIRELESS_FUOTA_TASK_TAGGED

**Resource Types:** AWS::IoTWireless::FuotaTask

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotwireless-multicast-group-tagged

Checks if AWS IoT Wireless multicast groups have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTWIRELESS_MULTICAST_GROUP_TAGGED

**Resource Types:** AWS::IoTWireless::MulticastGroup

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iotwireless-service-profile-tagged

Checks if AWS IoT Wireless service profiles have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOTWIRELESS_SERVICE_PROFILE_TAGGED

**Resource Types:** AWS::IoTWireless::ServiceProfile

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Sydney) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iot-authorizer-token-signing-enabled

Checks if an AWS IoT Core authorizer has not disabled the signing requirements for validating the token signature in an authorization request. The rule is NON_COMPLIANT if the authorizer has configuration.SigningDisabled set to True.

**Identifier:** IOT_AUTHORIZER_TOKEN_SIGNING_ENABLED

**Resource Types:** AWS::IoT::Authorizer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iot-job-template-tagged

Checks if AWS IoT job template resources resources have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOT_JOB_TEMPLATE_TAGGED

**Resource Types:** AWS::IoT::JobTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iot-provisioning-template-description

Checks if AWS IoT provisioning templates have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** IOT_PROVISIONING_TEMPLATE_DESCRIPTION

**Resource Types:** AWS::IoT::ProvisioningTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iot-provisioning-template-jitp

Checks if AWS IoT provisioning templates are using just-in-time provisioning (JITP). The rule is NON_COMPLIANT if configuration.TemplateType is not 'JITP'.

**Identifier:** IOT_PROVISIONING_TEMPLATE_JITP

**Resource Types:** AWS::IoT::ProvisioningTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iot-provisioning-template-tagged

Checks if AWS IoT provisioning templates have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOT_PROVISIONING_TEMPLATE_TAGGED

**Resource Types:** AWS::IoT::ProvisioningTemplate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## iot-scheduled-audit-tagged

Checks if AWS IoT scheduled audits have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IOT_SCHEDULED_AUDIT_TAGGED

**Resource Types:** AWS::IoT::ScheduledAudit

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Middle East (Bahrain), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Middle East (UAE), Europe (Frankfurt), Asia Pacific (Hong Kong), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ivs-channel-playback-authorization-enabled

Checks if Amazon IVS channels have playback authorization enabled. The rule is NON_COMPLIANT if configuration.Authorized is false.

**Identifier:** IVS_CHANNEL_PLAYBACK_AUTHORIZATION_ENABLED

**Resource Types:** AWS::IVS::Channel

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ivs-channel-tagged

Checks if Amazon IVS channels have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IVS_CHANNEL_TAGGED

**Resource Types:** AWS::IVS::Channel

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ivs-playback-key-pair-tagged

Checks if Amazon IVS playback key pairs have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IVS_PLAYBACK_KEY_PAIR_TAGGED

**Resource Types:** AWS::IVS::PlaybackKeyPair

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ivs-recording-configuration-tagged

Checks if Amazon IVS recording configurations have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** IVS_RECORDING_CONFIGURATION_TAGGED

**Resource Types:** AWS::IVS::RecordingConfiguration

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Tokyo), US West (Oregon) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## kinesis-firehose-delivery-stream-encrypted

Checks if Amazon Kinesis Data Firehose delivery streams are encrypted at rest with server-side encryption. The rule is NON_COMPLIANT if a Kinesis Data Firehose delivery stream is not encrypted at rest with server-side encryption.

**Identifier:** KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

**Resource Types:** AWS::KinesisFirehose::DeliveryStream

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of KMS Key Arns that are approved for Kinesis Firehose usage.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## kinesis-stream-backup-retention-check

Checks if an Amazon Kinesis Data Stream has its data record retention period set to a specific number of hours. The rule is NON_COMPLIANT if the property `RetentionPeriodHours` is set to a value less than the value specified by the parameter.

**Identifier:** KINESIS_STREAM_BACKUP_RETENTION_CHECK

**Resource Types:** AWS::Kinesis::Stream

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

minimumBackupRetentionPeriod (Optional), Type: String

Minimum hours data records should be retained. Valid values are 24 to 8760, default value is 168.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## kinesis-stream-encrypted

Checks if Amazon Kinesis streams are encrypted at rest with server-side encryption. The rule is NON_COMPLIANT for a Kinesis stream if 'StreamEncryption' is not present.

**Context**: Server-side encryption is a feature in Amazon Kinesis Data Streams that automatically encrypts data before it's at rest by using an AWS KMS Key. Data is encrypted before it's written to the Kinesis stream storage layer, and decrypted after it's retrieved from storage. As a result,

your data is encrypted at rest within the Kinesis Data Streams service. This can help you to meet regulatory requirements and enhance the security of your data. For more information, Data Protection in Amazon Kinesis Data Streams.

**Identifier:** KINESIS_STREAM_ENCRYPTED

**Resource Types:** AWS::Kinesis::Stream

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## kinesis-video-stream-minimum-data-retention

Checks if an Amazon Kinesis Video stream is configured with a value greater than or equal to the specified minimum data retention. The rule is NON_COMPLIANT if DataRetentionInHours is less than the value specified in the required rule parameter.

**Identifier:** KINESIS_VIDEO_STREAM_MINIMUM_DATA_RETENTION

**Resource Types:** AWS::KinesisVideo::Stream

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), Asia Pacific (Hong Kong), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

minDataRetentionInHours, Type: int

The minimum data retention in hours of the Amazon Kinesis Video stream for the rule to check. The rule is NON_COMPLIANT if the data retention in hours is less than the value specified in this parameter. Valid values are 0 to 87600.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## kms-cmk-not-scheduled-for-deletion

Checks if AWS Key Management Service (AWS KMS) keys are not scheduled for deletion in AWS KMS. The rule is NON_COMPLIANT if KMS keys are scheduled for deletion.

**Identifier:** KMS_CMK_NOT_SCHEDULED_FOR_DELETION

**Resource Types:** AWS::KMS::Key

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Europe (Milan), Asia Pacific (Taipei) Region

**Parameters:**

kmsKeyIds (Optional), Type: String

(Optional) Comma-separated list of specific customer managed key IDs not to be scheduled for deletion. If you do not specify any keys, the rule checks all the keys.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## kms-key-policy-no-public-access

Checks if the AWS KMS key policy allows public access. The rule is NON_COMPLIANT if the KMS key policy allows public access to the KMS key.

> **Note**
>
> To be considered non-public, a KMS key policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

**Identifier:** KMS_KEY_POLICY_NO_PUBLIC_ACCESS

**Resource Types:** AWS::KMS::Key

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## kms-key-tagged

Checks if AWS Key Management Service (KMS) keys have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** KMS_KEY_TAGGED

**Resource Types:** AWS::KMS::Key

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-concurrency-check

Checks if the Lambda function is configured with a function-level concurrent execution limit. The rule is NON_COMPLIANT if the Lambda function is not configured with a function-level concurrent execution limit.

**Identifier:** LAMBDA_CONCURRENCY_CHECK

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

ConcurrencyLimitHigh (Optional), Type: String

Maximum concurrency execution limit

ConcurrencyLimitLow (Optional), Type: String

Minimum concurrency execution limit

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-dlq-check

Checks whether an AWS Lambda function is configured with a dead-letter queue. The rule is NON_COMPLIANT if the Lambda function is not configured with a dead-letter queue.

**Identifier:** LAMBDA_DLQ_CHECK

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), China (Ningxia) Region

**Parameters:**

dlqArns (Optional), Type: CSV

Comma-separated list of Amazon SQS and Amazon SNS ARNs that must be configured as the Lambda function dead-letter queue target

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-function-description

Checks if AWS Lambda functions have a description. The rule is NON_COMPLIANT if configuration.description does not exist or is an empty string.

**Identifier:** LAMBDA_FUNCTION_DESCRIPTION

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-function-public-access-prohibited

Checks if the AWS Lambda function policy attached to the Lambda resource prohibits public access. If the Lambda function policy allows public access it is NON_COMPLIANT.

**Context**: A lambda function policy is considered to allow public access if the principal element is empty or contains a wildcard. For example, if the principal element is `“”` or `{“AWS”: “”}`. Granting public access is not recommended for security reasons. Restricting public access can help you prevent unauthorized invocations of your Lambda functions, which could compromise your data or incur unwanted costs.

To restrict access to your Lambda functions, specify the AWS account IDs or the Amazon Resource Names (ARNs) of the IAM users, roles, or services that can invoke the functions. For more information, see Granting function access to other accounts in the *AWS Lambda Developer Guide*.

The rule is also `NON_COMPLIANT` if a Lambda function is invoked from Amazon S3, and the policy doesn't include a condition to limit public access, such as `AWS:SourceAccount`. We recommend using other S3 conditions along with `AWS:SourceAccount` in your bucket policy for more refined access.

> **Note**
>
> To be considered non-public, a Lambda resource-based policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

**Identifier:** LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Spain), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-function-settings-check

Checks if the AWS Lambda function settings for runtime, role, timeout, and memory size match the expected values. The rule ignores functions with the 'Image' package type and functions with runtime set to 'OS-only Runtime'. The rule is NON_COMPLIANT if the Lambda function settings do not match the expected values.

**Identifier:** LAMBDA_FUNCTION_SETTINGS_CHECK

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

runtime, Type: CSV

Comma-separated list of AWS Lambda runtime values

role (Optional), Type: String

Name or ARN of the AWS Lambda execution role

memorySize (Optional), Type: int, Default: 128

AWS Lambda function size in megabytes

timeout (Optional), Type: int, Default: 3

AWS Lambda function timeout in seconds

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

*For more information on valid values for these inputs, see MemorySize, Role, Runtime, and Timeout in the AWS CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-function-xray-enabled

Checks if AWS X-Ray is enabled on AWS Lambda functions.The rule is NON_COMPLIANT if X-Ray tracing is disabled for a Lambda function.

**Identifier:** LAMBDA_FUNCTION_XRAY_ENABLED

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-inside-vpc

Checks if a Lambda function is allowed access to a virtual private cloud (VPC). The rule is NON_COMPLIANT if the Lambda function is not VPC enabled.

**Identifier:** LAMBDA_INSIDE_VPC

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

subnetIds (Optional), Type: CSV

Comma-separated list of subnet IDs that Lambda functions must be associated with.

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
```

```
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lambda-vpc-multi-az-check

Checks if Lambda has more than 1 availability zone associated. The rule is NON_COMPLIANT if only 1 availability zone is associated with the Lambda or the number of availability zones associated is less than number specified in the optional parameter.

**Identifier:** LAMBDA_VPC_MULTI_AZ_CHECK

**Resource Types:** AWS::Lambda::Function

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

availabilityZones (Optional), Type: int

Number of expected Availability zones.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lightsail-bucket-allow-public-overrides-disabled

Checks if Amazon Lightsail buckets have allow public overrides disabled. The rule is NON_COMPLIANT if AllowPublicOverrides is true. Note: AllowPublicOverrides has no effect if GetObject is public, see lightsail-bucket-get-object-private.

**Identifier:** LIGHTSAIL_BUCKET_ALLOW_PUBLIC_OVERRIDES_DISABLED

**Resource Types:** AWS::Lightsail::Bucket

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lightsail-bucket-tagged

Checks if Amazon Lightsail buckets have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** LIGHTSAIL_BUCKET_TAGGED

**Resource Types:** AWS::Lightsail::Bucket

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lightsail-certificate-tagged

Checks if Amazon Lightsail certificates have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** LIGHTSAIL_CERTIFICATE_TAGGED

**Resource Types:** AWS::Lightsail::Certificate

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## lightsail-disk-tagged

Checks if Amazon Lightsail disks have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** LIGHTSAIL_DISK_TAGGED

**Resource Types:** AWS::Lightsail::Disk

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## macie-auto-sensitive-data-discovery-check

Checks if automated sensitive data discovery is enabled for Amazon Macie. The rule is NON_COMPLIANT if automated sensitive data discovery is disabled. The rule is APPLICABLE for administrator accounts and NOT_APPLICABLE for member accounts.

**Identifier:** MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## macie-status-check

Checks if Amazon Macie is enabled in your account per region. The rule is NON_COMPLIANT if the 'status' attribute is not set to 'ENABLED'.

**Identifier:** MACIE_STATUS_CHECK

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mariadb-publish-logs-to-cloudwatch-logs

Checks if Amazon MariaDB database instances are configured to publish logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if a database instance is not configured to publish logs to CloudWatch Logs.

**Identifier:** MARIADB_PUBLISH_LOGS_TO_CLOUDWATCH_LOGS

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

logTypes (Optional), Type: String

Comma-separated list of log types for the rule to check. If not provided, the rule checks for the default log types: 'error' and 'audit'.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mfa-enabled-for-iam-console-access

Checks if AWS multi-factor authentication (MFA) is enabled for all AWS Identity and Access Management (IAM) users that use a console password. The rule is COMPLIANT if MFA is enabled.

> **Note**
>
> **Re-evaluation Timeline**
> Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by

AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

**Resource Types:** AWS::IAM::User

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-active-broker-ldap-authentication

Checks if Amazon MQ ActiveMQ brokers use the LDAP authentication strategy to secure the broker. The rule is NON_COMPLIANT if configuration.AuthenticationStrategy is not 'ldap'.

**Identifier:** MQ_ACTIVE_BROKER_LDAP_AUTHENTICATION

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-active-deployment-mode

Checks the deployment mode configured for Amazon MQ ActiveMQ broker engine. The rule is NON_COMPLIANT if the default single-instance broker mode is being used.

**Identifier:** MQ_ACTIVE_DEPLOYMENT_MODE

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-active-single-instance-broker-storage-type-efs

Checks if an Amazon MQ for ActiveMQ single-instance broker using the mq.m5 instance type family is configured with Amazon Elastic File System (EFS) for broker storage. The rule is NON_COMPLIANT if configuration.StorageType is not 'efs'.

**Identifier:** MQ_ACTIVE_SINGLE_INSTANCE_BROKER_STORAGE_TYPE_EFS

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-automatic-minor-version-upgrade-enabled

Checks if automatic minor version upgrades are enabled for Amazon MQ brokers. The rule is NON_COMPLIANT if the 'AutoMinorVersionUpgrade' field is not enabled for an Amazon MQ broker.

**Identifier:** MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central),

Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-auto-minor-version-upgrade-enabled

Checks if automatic minor version upgrades are enabled for Amazon MQ brokers. The rule is NON_COMPLIANT if the 'AutoMinorVersionUpgrade' field is not enabled for an Amazon MQ broker.

**Identifier:** MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-broker-general-logging-enabled

Checks if Amazon MQ brokers have general logging enabled. The rule is NON_COMPLIANT if configuration.Logs.General is false.

**Identifier:** MQ_BROKER_GENERAL_LOGGING_ENABLED

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-cloudwatch-audit-logging-enabled

Checks if Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled.

**Identifier:** MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-cloudwatch-audit-log-enabled

Checks if an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled.

**Identifier:** MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-no-public-access

Checks if Amazon MQ brokers are not publicly accessible. The rule is NON_COMPLIANT if the 'PubliclyAccessible' field is set to true for an Amazon MQ broker.

**Identifier:** MQ_NO_PUBLIC_ACCESS

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## mq-rabbit-deployment-mode

Checks the deployment mode configured for the Amazon MQ RabbitMQ broker engine. The rule is NON_COMPLIANT if the default single-instance broker mode is being used.

**Identifier:** MQ_RABBIT_DEPLOYMENT_MODE

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## msk-cluster-public-access-disabled

Checks if public access is disabled on Amazon MSK clusters. The rule is NON_COMPLIANT if public access on an Amazon MSK cluster is not disabled.

**Identifier:** MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

**Resource Types:** AWS::MSK::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## msk-cluster-tagged

Checks if Amazon MSK clusters have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** MSK_CLUSTER_TAGGED

**Resource Types:** AWS::MSK::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### msk-connect-connector-logging-enabled

Checks if Amazon MSK Connector has logging enabled to any one of the log destinations. The rule is NON_COMPLIANT if Amazon MSK Connector does not have logging enabled.

**Identifier:** MSK_CONNECT_CONNECTOR_LOGGING_ENABLED

**Resource Types:** AWS::KafkaConnect::Connector

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### msk-enhanced-monitoring-enabled

Checks if enhanced monitoring is enabled for an Amazon MSK cluster set to PER_TOPIC_PER_BROKER or PER_TOPIC_PER_PARTITION. The rule is NON_COMPLIANT if enhanced monitoring is enabled and set to DEFAULT or PER_BROKER.

**Identifier:** MSK_ENHANCED_MONITORING_ENABLED

**Resource Types:** AWS::MSK::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## msk-in-cluster-node-require-tls

Checks if an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections.

**Identifier:** MSK_IN_CLUSTER_NODE_REQUIRE_TLS

**Resource Types:** AWS::MSK::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## msk-unrestricted-access-check

Checks if an Amazon MSK Cluster has unauthenticated access disabled. The rule is NON_COMPLIANT if Amazon MSK Cluster has unauthenticated access enabled.

**Identifier:** MSK_UNRESTRICTED_ACCESS_CHECK

**Resource Types:** AWS::MSK::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## multi-region-cloudtrail-enabled

> **Important**
>
> For this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different.

Checks if there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the `ExcludeManagementEventSources` field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events.

**Identifier:** MULTI_REGION_CLOUD_TRAIL_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

s3BucketName (Optional), Type: String

Name of Amazon S3 bucket for AWS CloudTrail to deliver log files to.

snsTopicArn (Optional), Type: String

Amazon SNS topic ARN for AWS CloudTrail to use for notifications.

cloudWatchLogsLogGroupArn (Optional), Type: String

Amazon CloudWatch log group ARN for AWS CloudTrail to send data to.

includeManagementEvents (Optional), Type: boolean

Event selector to include management events for the AWS CloudTrail.

readWriteType (Optional), Type: String

Type of events to record. Valid values are ReadOnly, WriteOnly and ALL.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## nacl-no-unrestricted-ssh-rdp

Checks if default ports for SSH/RDP ingress traffic for network access control lists (NACLs) is unrestricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389.

**Identifier:** NACL_NO_UNRESTRICTED_SSH_RDP

**Resource Types:** AWS::EC2::NetworkAcl

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## neptune-cluster-backup-retention-check

Checks if an Amazon Neptune DB cluster retention period is set to specific number of days. The rule is NON_COMPLIANT if the retention period is less than the value specified by the parameter.

**Identifier:** NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

minimumBackupRetentionPeriod (Optional), Type: int

> Minimum days backups should be kept. Valid values 1 to 35, default value is 7. The rule is NON_COMPLIANT if value is greater than 'backupRetentionPeriod'. The rule is COMPLIANT if value is less than or equal to 'backupRetentionPeriod'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## neptune-cluster-cloudwatch-log-export-enabled

Checks if an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs.

**Identifier:** NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## neptune-cluster-copy-tags-to-snapshot-enabled

Checks if an Amazon Neptune cluster is configured to copy all tags to snapshots when the snapshots are created. The rule is NON_COMPLIANT if 'copyTagsToSnapshot' is set to false.

**Identifier:** NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan),

AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## neptune-cluster-deletion-protection-enabled

Checks if an Amazon Neptune DB cluster has deletion protection enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster has the deletionProtection field set to false.

**Identifier:** NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## neptune-cluster-encrypted

Checks if storage encryption is enabled for your Amazon Neptune DB clusters. The rule is NON_COMPLIANT if storage encryption is not enabled.

**Identifier:** NEPTUNE_CLUSTER_ENCRYPTED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

KmsKeyArns (Optional), Type: CSV

A comma-separated list of KMS key ARNs to compare with the KmsKeyId of the encrypted cluster.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## neptune-cluster-iam-database-authentication

Checks if an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled.

**Identifier:** NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### neptune-cluster-multi-az-enabled

Checks if an Amazon Neptune cluster is configured with Amazon RDS Multi-AZ replication. The rule is NON_COMPLIANT if Multi-AZ replication is not enabled.

**Identifier:** NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### neptune-cluster-snapshot-encrypted

Checks if an Amazon Neptune DB cluster has snapshots encrypted. The rule is NON_COMPLIANT if a Neptune cluster does not have snapshots encrypted.

**Identifier:** NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

**Resource Types:** AWS::RDS::DBClusterSnapshot

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## neptune-cluster-snapshot-public-prohibited

Checks if an Amazon Neptune manual DB cluster snapshot is public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public.

**Identifier:** NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

**Resource Types:** AWS::RDS::DBClusterSnapshot

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## netfw-deletion-protection-enabled

Checks if AWS Network Firewall has deletion protection enabled. The rule is NON_COMPLIANT if Network Firewall does not have deletion protection enabled.

**Identifier:** NETFW_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::NetworkFirewall::Firewall

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## netfw-logging-enabled

Checks if AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check.

**Identifier:** NETFW_LOGGING_ENABLED

**Resource Types:** AWS::NetworkFirewall::LoggingConfiguration

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

logType (Optional), Type: String

logType (Optional): Log type for the rule to check for firewalls: 'alert', 'flow', or 'both'.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### netfw-multi-az-enabled

Checks if AWS Network Firewall firewalls are deployed across multiple Availability Zones. The rule is NON_COMPLIANT if firewalls are deployed in only one Availability Zone or in fewer zones than the number listed in the optional parameter.

**Identifier:** NETFW_MULTI_AZ_ENABLED

**Resource Types:** AWS::NetworkFirewall::Firewall

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

availabilityZones (Optional), Type: int

The number of expected Availability Zones.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### netfw-policy-default-action-fragment-packets

Checks if an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action.

**Identifier:** NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

**Resource Types:** AWS::NetworkFirewall::FirewallPolicy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

statelessFragmentDefaultActions, Type: CSV

Comma-separated list of values. You can select a max of two. Valid values include 'aws:pass', 'aws:drop', and 'aws:forward_to_sfe'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## netfw-policy-default-action-full-packets

Checks if an AWS Network Firewall policy is configured with a user defined default stateless action for full packets. This rule is NON_COMPLIANT if default stateless action for full packets does not match with user defined default stateless action.

**Identifier:** NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

**Resource Types:** AWS::NetworkFirewall::FirewallPolicy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

statelessDefaultActions, Type: CSV

Comma-separated list of values. You can select a max of two. Valid values include 'aws:pass', 'aws:drop', and 'aws:forward_to_sfe'.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## netfw-policy-rule-group-associated

Check AWS Network Firewall policy is associated with stateful OR stateless rule groups. This rule is NON_COMPLIANT if no stateful or stateless rule groups are associated with the Network Firewall policy else COMPLIANT if any one of the rule group exists.

**Identifier:** NETFW_POLICY_RULE_GROUP_ASSOCIATED

**Resource Types:** AWS::NetworkFirewall::FirewallPolicy

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## netfw-stateless-rule-group-not-empty

Checks if a Stateless Network Firewall Rule Group contains rules. The rule is NON_COMPLIANT if there are no rules in a Stateless Network Firewall Rule Group.

**Identifier:** NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

**Resource Types:** AWS::NetworkFirewall::RuleGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## netfw-subnet-change-protection-enabled

Checks if AWS Network Firewall has subnet change protection enabled. The rule is NON_COMPLIANT if subnet change protection is not enabled.

**Identifier:** NETFW_SUBNET_CHANGE_PROTECTION_ENABLED

**Resource Types:** AWS::NetworkFirewall::Firewall

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## nlb-cross-zone-load-balancing-enabled

Checks if cross-zone load balancing is enabled on Network Load Balancers (NLBs). The rule is NON_COMPLIANT if cross-zone load balancing is not enabled for an NLB.

**Identifier:** NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## nlb-internal-scheme-check

Checks if a Network Load Balancer scheme is internal. The rule is NON_COMPLIANT if configuration.scheme is not set to internal.

**Identifier:** NLB_INTERNAL_SCHEME_CHECK

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## nlb-listener-tagged

Checks if Network Load Balancer listeners have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** NLB_LISTENER_TAGGED

**Resource Types:** AWS::ElasticLoadBalancingV2::Listener

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## nlb-logging-enabled

Checks if access logging is enabled for Network Load Balancers. The rule is NON_COMPLIANT if access logging is not enabled for a Network Load balancer.

**Identifier:** NLB_LOGGING_ENABLED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## nlb-tagged

Checks if Network Load Balancers have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** NLB_TAGGED

**Resource Types:** AWS::ElasticLoadBalancingV2::LoadBalancer

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## no-unrestricted-route-to-igw

Checks if there are public routes in the route table to an Internet gateway (IGW). The rule is NON_COMPLIANT if a route to an IGW has a destination CIDR block of '0.0.0.0/0' or '::/0' or if a destination CIDR block does not match the rule parameter.

**Identifier:** NO_UNRESTRICTED_ROUTE_TO_IGW

**Resource Types:** AWS::EC2::RouteTable

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

routeTableIds (Optional), Type: CSV

Comma-separated list of route table IDs that can have routes to an Internet Gateway with a destination CIDR block of '0.0.0.0/0' or '::/0'.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-access-control-enabled

Checks if Amazon OpenSearch Service domains have fine-grained access control enabled. The rule is NON_COMPLIANT if AdvancedSecurityOptions is not enabled for the OpenSearch Service domain.

**Identifier:** OPENSEARCH_ACCESS_CONTROL_ENABLED

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-audit-logging-enabled

Checks if Amazon OpenSearch Service domains have audit logging enabled. The rule is NON_COMPLIANT if an OpenSearch Service domain does not have audit logging enabled.

**Identifier:** OPENSEARCH_AUDIT_LOGGING_ENABLED

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

cloudWatchLogsLogGroupArnList (Optional), Type: CSV

> Comma-separated list of Amazon Resource Names (ARNs) for Amazon CloudWatch Logs log groups. The rule checks if the specified log groups are configured for audit logs.
>
> Valid values include: `arn:aws:logs:region:account-id:log-group:log_group_name:*` and `arn:aws:logs:region:account-id:log-group:log_group_name`.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-data-node-fault-tolerance

Checks if Amazon OpenSearch Service domains are configured with at least three data nodes and zoneAwarenessEnabled is true. The rule is NON_COMPLIANT for an OpenSearch domain if 'instanceCount' is less than 3 or 'zoneAwarenessEnabled' is set to 'false'.

**Identifier:** OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-encrypted-at-rest

Checks if Amazon OpenSearch Service domains have encryption at rest configuration enabled. The rule is NON_COMPLIANT if the `EncryptionAtRestOptions` field is not enabled.

> **Note**
>
> The rule does not evaluate Elasticsearch domains.

**Identifier:** OPENSEARCH_ENCRYPTED_AT_REST

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-https-required

Checks whether connections to OpenSearch domains are using HTTPS. The rule is NON_COMPLIANT if the Amazon OpenSearch domain 'EnforceHTTPS' is not 'true' or is 'true' and 'TLSSecurityPolicy' is not in '`tlsPolicies`'.

**Identifier:** OPENSEARCH_HTTPS_REQUIRED

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

tlsPolicies (Optional), Type: CSV

Comma-separated list of TLS security policies to check against the Amazon OpensSearch domain.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### opensearch-in-vpc-only

Checks if Amazon OpenSearch Service domains are in an Amazon Virtual Private Cloud (VPC). The rule is NON_COMPLIANT if an OpenSearch Service domain endpoint is public.

> **Note**
>
> The rule does not evaluate Elasticsearch domains.

**Identifier:** OPENSEARCH_IN_VPC_ONLY

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-logs-to-cloudwatch

Checks if Amazon OpenSearch Service domains are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if logging is not configured.

> **Note**
>
> The rule does not evaluate Elasticsearch domains.

**Identifier:** OPENSEARCH_LOGS_TO_CLOUDWATCH

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

logTypes (Optional), Type: CSV

Comma-separated list of logs that are enabled. Valid values are 'search', 'index', 'error'.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-node-to-node-encryption-check

Check if Amazon OpenSearch Service nodes are encrypted end to end. The rule is NON_COMPLIANT if the node-to-node encryption is not enabled on the domain

> **Note**
>
> The rule does not evaluate Elasticsearch domains.

**Identifier:** OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-primary-node-fault-tolerance

Checks if Amazon OpenSearch Service domains are configured with at least three dedicated primary nodes. The rule is NON_COMPLIANT for an OpenSearch Service domain if 'DedicatedMasterEnabled' is set to 'false', or 'DedicatedMasterCount' is less than 3.

**Identifier:** OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## opensearch-update-check

Checks if Amazon OpenSearch Service version updates are available but not installed. The rule is NON_COMPLIANT for an OpenSearch domain if the latest software updates are not installed.

**Identifier:** OPENSEARCH_UPDATE_CHECK

**Resource Types:** AWS::OpenSearch::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rabbit-mq-supported-version

Checks if an Amazon MQ RabbitMQ broker is running on a specified minimum supported engine version. The rule is NON_COMPLIANT if the RabbitMQ broker is not running on the minimum supported engine version that you specify.

**Identifier:** RABBIT_MQ_SUPPORTED_VERSION

**Resource Types:** AWS::AmazonMQ::Broker

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

supportedEngineVersion, Type: String

String value for the rule to check the minimum supported engine version for the RabbitMQ broker. RabbitMQ brokers use semantic versioning specification: X.Y.Z. X denotes the major version, Y represents the minor version, and Z denotes the patch version.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-aurora-mysql-audit-logging-enabled

Checks if Amazon Aurora MySQL-Compatible Edition clusters are configured to publish audit logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if Aurora MySQL-Compatible Edition clusters do not have audit log publishing configured.

**Identifier:** RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-aurora-postgresql-logs-to-cloudwatch

Checks if an Amazon Aurora PostgreSQL DB cluster is configured to publish PostgreSQL logs to Amazon CloudWatch Logs. This rule is NON_COMPLIANT if the DB cluster is not configured to publish PostgreSQL logs to Amazon CloudWatch Logs.

**Identifier:** RDS_AURORA_POSTGRESQL_LOGS_TO_CLOUDWATCH

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-automatic-minor-version-upgrade-enabled

Checks if Amazon Relational Database Service (RDS) database instances are configured for automatic minor version upgrades. The rule is NON_COMPLIANT if the value of 'autoMinorVersionUpgrade' is false.

**Identifier:** RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

*For more information on valid values for these inputs, see AutoMinorVersionUpgrade and Engine in the AWS CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-cluster-auto-minor-version-upgrade-enable

Checks if automatic minor version upgrades are enabled for Amazon RDS Multi-AZ cluster deployments. The rule is NON_COMPLIANT if autoMinorVersionUpgrade is set to false.

**Identifier:** RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), US West (N. California), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-cluster-default-admin-check

Checks if an Amazon Relational Database Service (Amazon RDS) database cluster has changed the admin username from its default value. The rule is NON_COMPLIANT if the admin username is set to the default value.

**Identifier:** RDS_CLUSTER_DEFAULT_ADMIN_CHECK

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

validAdminUserNames (Optional), Type: CSV

Comma-separated list of admin username(s) that Amazon RDS clusters can use. Cannot include 'postgres' or 'admin' as valid username(s) as these are default values.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-cluster-deletion-protection-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) cluster has deletion protection enabled. This rule is NON_COMPLIANT if an RDS cluster does not have deletion protection enabled.

**Identifier:** RDS_CLUSTER_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-cluster-encrypted-at-rest

Checks if an Amazon Relational Database Service (Amazon RDS) cluster is encrypted at rest. The rule is NON_COMPLIANT if an Amazon RDS cluster is not encrypted at rest.

**Identifier:** RDS_CLUSTER_ENCRYPTED_AT_REST

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-cluster-iam-authentication-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled.

**Identifier:** RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-cluster-multi-az-enabled

Checks if Multi-Availability Zone (Multi-AZ) replication is enabled on Amazon Aurora and Multi-AZ DB clusters managed by Amazon Relational Database Service (Amazon RDS). The rule is NON_COMPLIANT if an Amazon RDS instance is not configured with Multi-AZ.

**Identifier:** RDS_CLUSTER_MULTI_AZ_ENABLED

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-db-security-group-not-allowed

Checks if there are any Amazon Relational Database Service (Amazon RDS) DB security groups that are not the default DB security group. The rule is NON_COMPLIANT if there are any DB security groups that are not the default DB security group.

**Identifier:** RDS_DB_SECURITY_GROUP_NOT_ALLOWED

**Resource Types:** AWS::RDS::DBSecurityGroup

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Ireland), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-enhanced-monitoring-enabled

Checks if enhanced monitoring is enabled for Amazon RDS instances. This rule is NON_COMPLIANT if '`monitoringInterval`' is '0' in the configuration item of the RDS instance, or if '`monitoringInterval`' does not match the rule parameter value.

**Identifier:** RDS_ENHANCED_MONITORING_ENABLED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

monitoringInterval (Optional), Type: int

An integer value in seconds between points when enhanced monitoring metrics are collected for the database instance. The valid values are 1, 5, 10, 15, 30, and 60.

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

*For more information on valid values for these inputs, see MonitoringInterval and Engine in the AWS CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-event-subscription-tagged

Checks if Amazon RDS event subscriptions have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** RDS_EVENT_SUBSCRIPTION_TAGGED

**Resource Types:** AWS::RDS::EventSubscription

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-instance-default-admin-check

Checks if an Amazon Relational Database Service (Amazon RDS) database has changed the admin username from its default value. This rule will only run on RDS database instances. The rule is NON_COMPLIANT if the admin username is set to the default value.

**Identifier:** RDS_INSTANCE_DEFAULT_ADMIN_CHECK

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

validAdminUserNames (Optional), Type: CSV

Comma-separated list of admin username(s) that Amazon RDS instances can use. (Cannot include 'postgres' or 'admin' as valid username(s) as these are default values.)

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-instance-deletion-protection-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) instance has deletion protection enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have deletion protection enabled; for example, deletionProtection is set to false.

> **Warning**
> Some RDS DB instances within a Cluster (Aurora/DocumentDB) will show as non-compliant.

**Identifier:** RDS_INSTANCE_DELETION_PROTECTION_ENABLED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

databaseEngines (Optional), Type: CSV

Comma-separated list of RDS database engines to include in the evaluation of the rule. For example, 'mysql, postgres, mariadb'.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### rds-instance-iam-authentication-enabled

Checks if an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled.

> **Note**
>
> The DB Engine should be one of 'mysql', 'postgres', 'aurora', 'aurora-mysql', or 'aurora-postgresql'. The DB instance status should be one of 'available', 'backing-up', 'storage-optimization', or 'storage-full'.

**Identifier:** RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-instance-public-access-check

Checks if the Amazon Relational Database Service (Amazon RDS) instances are not publicly accessible. The rule is NON_COMPLIANT if the publiclyAccessible field is true in the instance configuration item.

**Identifier:** RDS_INSTANCE_PUBLIC_ACCESS_CHECK

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-instance-subnet-igw-check

Checks if RDS DB instances are deployed in a public subnet with a route to the internet gateway. The rule is NON_COMPLIANT if RDS DB instances is deployed in a public subnet

**Identifier:** RDS_INSTANCE_SUBNET_IGW_CHECK

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-in-backup-plan

Checks if Amazon Relational Database Service (Amazon RDS) databases are present in AWS Backup plans. The rule is NON_COMPLIANT if Amazon RDS databases are not included in any AWS Backup plan.

> **Note**
>
> The rule only applies to Amazon Aurora DB instances. DB clusters are not supported.

**Identifier:** RDS_IN_BACKUP_PLAN

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon Relational Database Service (Amazon RDS). The rule is NON_COMPLIANT if the Amazon RDS instance does not have a corresponding recovery point created within the specified time period.

**Identifier:** RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon RDS instances for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Amazon RDS instance for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### rds-logging-enabled

Checks if respective logs of Amazon Relational Database Service (Amazon RDS) are enabled. The rule is NON_COMPLIANT if any log types are not enabled.

> **Note**
>
> DB Instances that are not in 'available', 'backing-up', 'storage-optimization', or 'storage-full' status evaluate as `NOT_APPLICABLE`.

**Identifier:** RDS_LOGGING_ENABLED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

additionalLogs (Optional), Type: StringMap

Comma-separated list of engine names and log type names. For example, "additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-mariadb-instance-encrypted-in-transit

Checks if connections to Amazon RDS for MariaDB DB instances with engine version greater than or equal to 10.5 use encryption in transit. The rule is NON_COMPLIANT if the DB parameter group is not in-sync or if require_secure_transport is not set to ON.

**Identifier:** RDS_MARIADB_INSTANCE_ENCRYPTED_IN_TRANSIT

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-meets-restore-time-target

Checks if the restore time of Amazon Relational Database Service (Amazon RDS) instances meets specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of an Amazon RDS instance is greater than maxRestoreTime minutes.

**Identifier:** RDS_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags of Amazon RDS instances for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Amazon RDS instance for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-multi-az-support

Checks whether high availability is enabled for your RDS DB instances.

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. For more information, see High Availability (Multi-AZ) in the *Amazon RDS User Guide*.

> **Note**
>
> This rule does not evaluate Amazon Aurora DB, Amazon DocumentDB, and Amazon Neptune DB instances.

**Identifier:** RDS_MULTI_AZ_SUPPORT

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

*For more information on valid values for these inputs, see MultiAZ and Engine in the AWS CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-mysql-cluster-copy-tags-to-snapshot-check

Checks if Amazon Relational Database Service (Amazon RDS) MySQL DB clusters are configured to copy tags to snapshots. The rule is NON_COMPLIANT if an Amazon RDS MySQL DB cluster is not configured to copy tags to snapshots.

**Identifier:** RDS_MYSQL_CLUSTER_COPY_TAGS_TO_SNAPSHOT_CHECK

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), US West (N. California), Asia Pacific (Taipei) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### rds-mysql-instance-encrypted-in-transit

Checks if connections to Amazon RDS for MySQL database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the associated database parameter group is not in-sync or if the require_secure_transport parameter is not set to 1.

> **Note**
>
> The rule returns `NOT_APPLICABLE` if the Amazon RDS instance is part of an RDS cluster.

**Identifier:** RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-option-group-tagged

Checks if Amazon RDS option group resources have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** RDS_OPTION_GROUP_TAGGED

**Resource Types:** AWS::RDS::OptionGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-pgsql-cluster-copy-tags-to-snapshot-check

Checks if Amazon Relational Database Service (Amazon RDS) PostgreSQL DB clusters are configured to copy tags to snapshots. The rule is NON_COMPLIANT if an RDS PostgreSQL DB cluster's CopyTagsToSnapshot property is set to false.

**Identifier:** RDS_PGSQL_CLUSTER_COPY_TAGS_TO_SNAPSHOT_CHECK

**Resource Types:** AWS::RDS::DBCluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), US West (N. California), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-postgresql-logs-to-cloudwatch

Checks if an Amazon PostgreSQL DB instance is configured to publish logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the DB instance is not configured to publish logs to Amazon CloudWatch Logs.

**Identifier:** RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

logTypes (Optional), Type: CSV

> Comma-separated list of log types to be published to CloudWatch Logs. Valid values are: 'postgresql', 'upgrade'. Default value is 'postgresql'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-postgres-instance-encrypted-in-transit

Checks if connections to Amazon RDS PostgreSQL database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the associated database parameter group is not in-sync or if the rds.force_ssl parameter is not set to 1.

> **Note**
>
> The rule returns `NOT_APPLICABLE` if the Amazon RDS instance is part of an RDS cluster.

**Identifier:** RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-proxy-tls-encryption

Checks if Amazon RDS proxies enforce TLS for all connections. The rule is NON_COMPLIANT if an Amazon RDS proxy does not have TLS enforced for all connections.

**Identifier:** RDS_PROXY_TLS_ENCRYPTION

**Resource Types:** AWS::RDS::DBProxy

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-resources-protected-by-backup-plan

Checks if Amazon Relational Database Service (Amazon RDS) instances are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon RDS Database instance is not covered by a backup plan.

**Identifier:** RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for Amazon RDS instances for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Amazon RDS instance for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-snapshots-public-prohibited

Checks if Amazon Relational Database Service (Amazon RDS) snapshots are public. The rule is NON_COMPLIANT if any existing and new Amazon RDS snapshots are public.

> **Note**
>
> It can take up to 12 hours for compliance results to be captured.

**Identifier:** RDS_SNAPSHOTS_PUBLIC_PROHIBITED

**Resource Types:** AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Africa (Cape Town), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### rds-snapshot-encrypted

Checks if Amazon Relational Database Service (Amazon RDS) DB snapshots are encrypted. The rule is NON_COMPLIANT if the Amazon RDS DB snapshots are not encrypted.

**Identifier:** RDS_SNAPSHOT_ENCRYPTED

**Resource Types:** AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### rds-sqlserver-encrypted-in-transit

Checks if connections to Amazon RDS SQL server database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the DB parameter force_ssl for the parameter group is not set to 1 or the ApplyStatus parameter is not 'in-sync'.

**Identifier:** RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-sql-server-logs-to-cloudwatch

Checks if an Amazon SQL Server DB instance is configured to publish logs to Amazon CloudWatch Logs. This rule is NON_COMPLIANT if the DB instance is not configured to publish logs to Amazon CloudWatch Logs.

**Identifier:** RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

logTypes (Optional), Type: CSV

> logTypes - (Optional): Comma-separated list of log types to be published to CloudWatch Logs. Valid values are: 'error', 'agent'. Default value is 'error', 'agent'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## rds-storage-encrypted

Checks if storage encryption is enabled for your Amazon Relational Database Service (Amazon RDS) DB instances. The rule is NON_COMPLIANT if storage encryption is not enabled.

**Identifier:** RDS_STORAGE_ENCRYPTED

**Resource Types:** AWS::RDS::DBInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

kmsKeyId (Optional), Type: String

KMS key ID or Amazon Resource Name (ARN) used to encrypt the storage.

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-audit-logging-enabled

Checks if Amazon Redshift clusters are logging audits to a specific bucket. The rule is NON_COMPLIANT if audit logging is not enabled for a Redshift cluster or if the '`bucketNames`' parameter is provided but the audit logging destination does not match.

**Identifier:** REDSHIFT_AUDIT_LOGGING_ENABLED

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

bucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names for storing audit logs.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-backup-enabled

Checks that Amazon Redshift automated snapshots are enabled for clusters. The rule is NON_COMPLIANT if the value for `automatedSnapshotRetentionPeriod` is greater than `MaxRetentionPeriod` or less than `MinRetentionPeriod` or the value is 0.

**Identifier:** REDSHIFT_BACKUP_ENABLED

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Mexico (Central) Region

**Parameters:**

MinRetentionPeriod (Optional), Type: int

Minimum value for the retention period. Minimum value is 1.

MaxRetentionPeriod (Optional), Type: int

Maximum value for the retention period. Maximum value is 35.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-cluster-configuration-check

Checks if Amazon Redshift clusters have the specified settings. The rule is NON_COMPLIANT if the Amazon Redshift cluster is not encrypted or encrypted with another key, or if a cluster does not have audit logging enabled.

**Identifier:** REDSHIFT_CLUSTER_CONFIGURATION_CHECK

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Mexico (Central) Region

**Parameters:**

loggingEnabled, Type: boolean, Default: true

Audit logging is enabled

clusterDbEncrypted, Type: boolean, Default: true

Database encryption is enabled

nodeTypes (Optional), Type: CSV, Default: dc1.large

Specify node type

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-cluster-kms-enabled

Checks if Amazon Redshift clusters are using a specified AWS Key Management Service (AWS KMS) key for encryption. The rule is COMPLIANT if encryption is enabled and the cluster is encrypted with the key provided in the `kmsKeyArn` parameter. The rule is NON_COMPLIANT if the cluster is not encrypted or encrypted with another key.

**Identifier:** REDSHIFT_CLUSTER_KMS_ENABLED

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of AWS KMS key Amazon Resource Names (ARNs) used in Amazon Redshift clusters for encryption.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-cluster-maintenancesettings-check

Checks if Amazon Redshift clusters have the specified maintenance settings. The rule is NON_COMPLIANT if the automatic upgrades to major version is disabled.

**Identifier:** REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Mexico (Central) Region

**Parameters:**

allowVersionUpgrade, Type: boolean, Default: true

Allow version upgrade is enabled.

preferredMaintenanceWindow (Optional), Type: String

Scheduled maintenance window for clusters (for example, Mon:09:30-Mon:10:00).

automatedSnapshotRetentionPeriod (Optional), Type: int, Default: 1

Number of days to retain automated snapshots.

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

*For more information on valid values for these inputs, see AutomatedSnapshotRetentionPeriod, PreferredMaintenanceWindow, and AllowVersionUpgrade in the AWS CloudFormation User Guide.

For more information on proactive evaluation, see Evaluation Mode.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-cluster-multi-az-enabled

Checks if an Amazon Redshift cluster has multiple Availability Zones deployments enabled. This rule is NON_COMPLIANT if Amazon Redshift cluster does not have multiple Availability Zones deployments enabled.

**Identifier:** REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Mexico (Central), US West (N. California), Asia Pacific (Taipei) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-cluster-parameter-group-tagged

Checks if Amazon Redshift cluster parameter groups have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** REDSHIFT_CLUSTER_PARAMETER_GROUP_TAGGED

**Resource Types:** AWS::Redshift::ClusterParameterGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### redshift-cluster-public-access-check

Checks whether Amazon Redshift clusters are not publicly accessible. The rule is NON_COMPLIANT if the publiclyAccessible field is true in the cluster configuration item.

**Identifier:** REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Stockholm), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

#### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
```

```
   "PubliclyAccessible": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-cluster-subnet-group-multi-az

Checks If Amazon Redshift subnet groups contain subnets from more than one Availability Zone. The rule is NON_COMPLIANT if an Amazon Redshift subnet group does not contain subnets from at least two different Availability Zones.

**Identifier:** REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

**Resource Types:** AWS::Redshift::ClusterSubnetGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-default-admin-check

Checks if an Amazon Redshift cluster has changed the admin username from its default value. The rule is NON_COMPLIANT if the admin username for a Redshift cluster is set to “awsuser” or if the username does not match what is listed in parameter.

**Identifier:** REDSHIFT_DEFAULT_ADMIN_CHECK

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

validAdminUserNames (Optional), Type: CSV

Comma-separated list of admin username(s) for Redshift clusters to use. Note: 'awsuser' is the default and not accepted.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-default-db-name-check

Checks if a Redshift cluster has changed its database name from the default value. The rule is NON_COMPLIANT if the database name for a Redshift cluster is set to “dev”, or if the optional parameter is provided and the database name does not match.

**Identifier:** REDSHIFT_DEFAULT_DB_NAME_CHECK

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

validDatabaseNames (Optional), Type: CSV

Comma-separated list of database name(s) for Redshift clusters.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-enhanced-vpc-routing-enabled

Checks if Amazon Redshift cluster has 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'.

**Identifier:** REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Europe (Stockholm), China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-require-tls-ssl

Checks if Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. The rule is NON_COMPLIANT if any Amazon Redshift cluster has parameter require_SSL not set to true.

**Identifier:** REDSHIFT_REQUIRE_TLS_SSL

**Resource Types:** AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Mexico (Central) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-serverless-default-admin-check

Checks if an Amazon Redshift Serverless Namespace has changed the admin username from its default value. The rule is NON_COMPLIANT if the admin username for a Redshift Serverless Namespace is set to “admin”.

**Identifier:** REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

**Resource Types:** AWS::RedshiftServerless::Namespace

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-serverless-default-db-name-check

Checks if an Amazon Redshift Serverless namespace has changed its database name from the default value. The rule is NON_COMPLIANT if the database name for an Amazon Redshift Serverless namespace is set to `dev`.

**Identifier:** REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

**Resource Types:** AWS::RedshiftServerless::Namespace

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-serverless-namespace-cmk-encryption

Checks if Amazon Redshift Serverless namespaces are encrypted by customer managed AWS KMS keys. The rule is NON_COMPLIANT if a namespace is not encrypted by a customer managed key. Optionally, you can specify a list of KMS keys for rule to check.

**Identifier:** REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

**Resource Types:** AWS::RedshiftServerless::Namespace

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of Amazon Resource Names (ARNs) of customer managed keys for the rule to check. If provided, the rule is NON_COMPLIANT if an Amazon Redshift Serverless namespace is not encrypted with one of these KMS keys.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-serverless-publish-logs-to-cloudwatch

Checks if Amazon Redshift Serverless Namespace is configured to publish the following logs to Amazon CloudWatch Logs. This rule is NON_COMPLIANT if the Namespace is not configured to publish the following logs to Amazon CloudWatch Logs.

**Identifier:** REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

**Resource Types:** AWS::RedshiftServerless::Namespace

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

logType (Optional), Type: CSV

Comma-separated list of log types to be published to CloudWatch Logs. Valid values are 'connectionlog', 'userlog' Default value is 'connectionlog', 'userlog'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-serverless-workgroup-encrypted-in-transit

Checks if AWS Redshift Serverless workgroups have the require_ssl config parameter set to true. The rule is NON_COMPLIANT if require_ssl is set to false.

**Identifier:** REDSHIFT_SERVERLESS_WORKGROUP_ENCRYPTED_IN_TRANSIT

**Resource Types:** AWS::RedshiftServerless::Workgroup

**Trigger type:** Periodic

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-serverless-workgroup-no-public-access

Checks if Amazon Redshift Serverless workgroups do not allow public access. The rule is NON_COMPLIANT if a workgroup has 'Turn on Public Accessible' enabled.

**Identifier:** REDSHIFT_SERVERLESS_WORKGROUP_NO_PUBLIC_ACCESS

**Resource Types:** AWS::RedshiftServerless::Workgroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-serverless-workgroup-routes-within-vpc

Checks if Amazon Redshift Serverless workgroups route the network traffic through a VPC. The rule is NON_COMPLIANT if workgroups have 'Turn on Enhanced VPC routing' disabled.

**Identifier:** REDSHIFT_SERVERLESS_WORKGROUP_ROUTES_WITHIN_VPC

**Resource Types:** AWS::RedshiftServerless::Workgroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Jakarta), Africa (Cape Town), Middle East (UAE), South America (Sao Paulo), Asia Pacific (Hong Kong), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Europe (Milan), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## redshift-unrestricted-port-access

Checks if security groups associated with an Amazon Redshift cluster have inbound rules that allow unrestricted incoming traffic. The rule is NON_COMPLIANT if there are inbound rules that allow unrestricted incoming traffic to the Redshift cluster port.

**Identifier:** REDSHIFT_UNRESTRICTED_PORT_ACCESS

**Resource Types:** AWS::Redshift::Cluster

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## required-tags

Checks if your resources have the tags that you specify. For example, you can check whether your Amazon EC2 instances have the `CostCenter` tag, while also checking if all your RDS instance have one set of Keys tag. Separate multiple values with commas. You can check up to 6 tags at a time.

The AWS-managed AWS Systems Manager automation document `AWS-SetRequiredTags` does not work as a remediation with this rule. You will need to create your own custom Systems Manager automation documentation for remediation.

**Context**: AWS allows you to assign metadata to AWS resources in the form of tags. Each tag is a label consisting of a key and an optional value to store information about the resource or data retained on that resource. For more information see, Building your tagging strategy.

You can use this rule to find resources in your account that were not launched with your desired configurations by specifying which resources should have tags and the expected value for each tag. You can also run remediation actions to fix tagging mistakes. However, this rule does not prevent you from creating resources with incorrect tags.

> **Note**
>
> AWS Config does not support recording associated tags for all resource types. To verify if AWS Config records tags in the configuration item (CI) for a specific resource type:

- Check that AWS Config correctly records the current configuration for the resource, excluding tags.
- Check that AWS Config refreshes the recorded configuration when a change is made to the resource.

**Identifier:** REQUIRED_TAGS

**Resource Types:** AWS::ACM::Certificate, AWS::AutoScaling::AutoScalingGroup, AWS::CloudFormation::Stack, AWS::CodeBuild::Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnetGroup, AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

tag1Key, Type: String, Default: CostCenter

Key of the required tag.

tag1Value (Optional), Type: CSV

Optional value of the required tag. Separate multiple values with commas.

tag2Key (Optional), Type: String

Key of a second required tag.

tag2Value (Optional), Type: CSV

Optional value of the second required tag. Separate multiple values with commas.

tag3Key (Optional), Type: String

Key of a third required tag.

tag3Value (Optional), Type: CSV

Optional value of the third required tag. Separate multiple values with commas.

tag4Key (Optional), Type: String

Key of a fourth required tag.

tag4Value (Optional), Type: CSV

Optional value of the fourth required tag. Separate multiple values with commas.

tag5Key (Optional), Type: String

Key of a fifth required tag.

tag5Value (Optional), Type: CSV

Optional value of the fifth required tag. Separate multiple values with commas.

tag6Key (Optional), Type: String

Key of a sixth required tag.

tag6Value (Optional), Type: CSV

Optional value of the sixth required tag. Separate multiple values with commas.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### restricted-common-ports

> **Important**
>
> For this rule, the rule identifier (RESTRICTED_INCOMING_TRAFFIC) and rule name (restricted-common-ports) are different.

Checks if the security groups in use do not allow unrestricted incoming Transmission Control Protocol (TCP) traffic to specified ports. The rule is COMPLIANT if:

- Port access is blocked to all TCP traffic.
- Port access is open to TCP traffic through Inbound rules, where the source is either a single IPv4 address or a range of IPv4 addresses in CIDR notation which does not cover all IPv4 addresses ("0.0.0.0/0").
- Port access is open to TCP traffic through Inbound rules, where the source is either a single IPv6 address or a range of IPv6 addresses in CIDR notation which does not cover all IPv6 addresses ("::/0)").

The rule is NON_COMPLIANT if IP addresses for inbound TCP connections are not restricted to specified ports.

**Identifier:** RESTRICTED_INCOMING_TRAFFIC

**Resource Types:** AWS::EC2::SecurityGroup

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

blockedPort1 (Optional), Type: int, Default: 20

Blocked TCP port number. The default of 20 corresponds to File Transfer Protocol (FTP) Data Transfer.

blockedPort2 (Optional), Type: int, Default: 21

Blocked TCP port number. The default of 21 corresponds to File Transfer Protocol (FTP) Command Control.

blockedPort3 (Optional), Type: int, Default: 3389

Blocked TCP port number. The default of 3389 corresponds to Remote Desktop Protocol (RDP).

blockedPort4 (Optional), Type: int, Default: 3306

Blocked TCP port number. The default of 3306 corresponds to MySQL protocol.

blockedPort5 (Optional), Type: int, Default: 4333

Blocked TCP port number. Used for a specific port relevant for your environment.

blockedPorts (Optional), Type: CSV

Comma-separated list of blocked TCP port numbers. For example: 20, 21, 3306, 3389.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### root-account-hardware-mfa-enabled

Checks if your AWS account is enabled to use multi-factor authentication (MFA) hardware device to sign in with root credentials. The rule is NON_COMPLIANT if any virtual MFA devices are permitted for signing in with root credentials.

> **Note**
>
> **Not Applicable for Accounts Without Root User Credentials**
> This rule returns `NOT_APPLICABLE` if root user credentials are not present.
> **Managed Rules and Global IAM Resource Types**
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## root-account-mfa-enabled

Checks if the root user of your AWS account requires multi-factor authentication for console sign-in. The rule is NON_COMPLIANT if the AWS Identity and Access Management (IAM) root account user does not have multi-factor authentication (MFA) enabled.

> **Note**
>
> **Not Applicable for Accounts Without Root User Credentials**
>
> This rule returns `NOT_APPLICABLE` if root user credentials are not present.
>
> **Managed Rules and Global IAM Resource Types**
>
> The global IAM resource types onboarded before February 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, and `AWS::IAM::User`) can only be recorded by AWS Config in AWS Regions where AWS Config was available before February 2022. These resource types cannot be recorded in Regions supported by AWS Config after February 2022. For a list of those Regions, see Recording AWS Resources | Global Resources.
>
> If you record a global IAM resource type in at least one Region, periodic rules that report compliance on the global IAM resource type will run evaluations in all Regions where the periodic rule is added, even if you have not enabled the recording of the global IAM resource type in the Region where the periodic rule was added.
>
> To avoid unnecessary evaluations, you should only deploy periodic rules that report compliance on a global IAM resource type to one of the supported Regions. For a list of

which managed rules are supported in which Regions, see List of AWS Config Managed Rules by Region Availability.

**Identifier:** ROOT_ACCOUNT_MFA_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## route53-health-check-tagged

Checks if Amazon Route 53 health checks have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ROUTE53_HEALTH_CHECK_TAGGED

**Resource Types:** AWS::Route53::HealthCheck

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## route53-hosted-zone-tagged

Checks if Amazon Route 53 hosted zones have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ROUTE53_HOSTED_ZONE_TAGGED

**Resource Types:** AWS::Route53::HostedZone

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## route53-query-logging-enabled

Checks if DNS query logging is enabled for your Amazon Route 53 public hosted zones. The rule is NON_COMPLIANT if DNS query logging is not enabled for your Amazon Route 53 public hosted zones.

**Identifier:** ROUTE53_QUERY_LOGGING_ENABLED

**Resource Types:** AWS::Route53::HostedZone

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## route53-resolver-firewall-domain-list-tagged

Checks if Amazon Route 53 Resolver firewall domain lists have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ROUTE53_RESOLVER_FIREWALL_DOMAIN_LIST_TAGGED

**Resource Types:** AWS::Route53Resolver::FirewallDomainList

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## route53-resolver-firewall-rule-group-association-tagged

Checks if Amazon Route 53 Resolver firewall rule group associations have tags. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ROUTE53_RESOLVER_FIREWALL_RULE_GROUP_ASSOCIATION_TAGGED

**Resource Types:** AWS::Route53Resolver::FirewallRuleGroupAssociation

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## route53-resolver-firewall-rule-group-tagged

Checks if Amazon Route 53 Resolver firewall rule groups have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ROUTE53_RESOLVER_FIREWALL_RULE_GROUP_TAGGED

**Resource Types:** AWS::Route53Resolver::FirewallRuleGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## route53-resolver-resolver-rule-tagged

Checks if Amazon Route 53 Resolver resolver rules have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** ROUTE53_RESOLVER_RESOLVER_RULE_TAGGED

**Resource Types:** AWS::Route53Resolver::ResolverRule

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### rum-app-monitor-cloudwatch-logs-enabled

Checks if Amazon CloudWatch RUM app monitors have CloudWatch logs enabled. The rule is NON_COMPLIANT if configuration.CwLogEnabled is false.

**Identifier:** RUM_APP_MONITOR_CLOUDWATCH_LOGS_ENABLED

**Resource Types:** AWS::RUM::AppMonitor

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hong Kong), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### rum-app-monitor-tagged

Checks if Amazon CloudWatch RUM app monitors have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** RUM_APP_MONITOR_TAGGED

**Resource Types:** AWS::RUM::AppMonitor

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Africa (Cape Town), Asia Pacific (Hong Kong), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3express-dir-bucket-lifecycle-rules-check

Checks if lifecycle rules are configured for an Amazon S3 Express directory bucket. The rule is NON_COMPLIANT if there is no active lifecycle configuration rules or the configuration does not match with the parameter values.

**Identifier:** S3EXPRESS_DIR_BUCKET_LIFECYCLE_RULES_CHECK

**Resource Types:** AWS::S3Express::DirectoryBucket

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Stockholm), Asia Pacific (Mumbai), US East (Ohio), Europe (Ireland), US East (N. Virginia), Asia Pacific (Tokyo), US West (Oregon) Region

**Parameters:**

targetExpirationDays (Optional), Type: int

Number of days after creation when objects are deleted from Amazon S3 Express directory buckets.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-access-point-in-vpc-only

Checks if an Amazon S3 access point does not allow access from the internet (NetworkOrigin is VPC). The rule is NON_COMPLIANT if NetworkOrigin is Internet.

**Identifier:** S3_ACCESS_POINT_IN_VPC_ONLY

**Resource Types:** AWS::S3::AccessPoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-access-point-public-access-blocks

Checks if Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points.

**Identifier:** S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

**Resource Types:** AWS::S3::AccessPoint

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

excludedAccessPoints (Optional), Type: CSV

Comma-separated list of names for allowed public Amazon S3 access points.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-account-level-public-access-blocks

Checks if the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item.

> **Note**
>
> If you are using this rule, ensure that S3 Block Public Access is enabled. The rule is change-triggered, so it will not be invoked unless S3 Block Public Access is enabled. If S3 Block Public Access is not enabled the rule returns INSUFFICIENT_DATA. This means that you still might have some public buckets. For more information about setting up S3 Block Public Access, see Blocking public access to your Amazon S3 storage.

**Identifier:** S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

**Resource Types:** AWS::S3::AccountPublicAccessBlock

**Trigger type:** Configuration changes (current status not checked, only evaluated when changes generate new events)

> **Note**
>
> This rule is only triggered by configuration changes for the specific region where the S3 endpoint is located. In all other regions, the rule is checked periodically. If a change was made in another region, there could be a delay before the rule returns NON_COMPLIANT.

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

RestrictPublicBuckets (Optional), Type: String, Default: True

RestrictPublicBuckets is enforced or not, default True

BlockPublicPolicy (Optional), Type: String, Default: True

BlockPublicPolicy is enforced or not, default True

BlockPublicAcls (Optional), Type: String, Default: True

BlockPublicAcls is enforced or not, default True

IgnorePublicAcls (Optional), Type: String, Default: True

IgnorePublicAcls is enforced or not, default True

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-account-level-public-access-blocks-periodic

Checks if the required public access block settings are configured at the account level. The rule is NON_COMPLIANT if the configuration item does not match one or more settings from parameters (or default).

**Identifier:** S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

IgnorePublicAcls (Optional), Type: String

IgnorePublicAcls is enforced or not, default True

BlockPublicPolicy (Optional), Type: String

BlockPublicPolicy is enforced or not, default True

BlockPublicAcls (Optional), Type: String

BlockPublicAcls is enforced or not, default True

RestrictPublicBuckets (Optional), Type: String

RestrictPublicBuckets is enforced or not, default True

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-acl-prohibited

Checks if Amazon Simple Storage Service (Amazon S3) Buckets allow user permissions through access control lists (ACLs). The rule is NON_COMPLIANT if ACLs are configured for user access in Amazon S3 Buckets.

**Identifier:** S3_BUCKET_ACL_PROHIBITED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-blacklisted-actions-prohibited

Checks if an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any `s3:GetBucket*` actions and `s3:DeleteObject` on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy.

> **Note**
>
> The rule will only check for entities in the Principal property and does not take into account any conditionals under the Condition property in a policy

**Identifier:** S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

blacklistedActionPattern, Type: CSV

Comma-separated list of blacklisted action patterns, for example, s3:GetBucket* and s3:DeleteObject.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-cross-region-replication-enabled

Checks if you have enabled S3 Cross-Region Replication for your Amazon S3 buckets. The rule is NON_COMPLIANT if there are no replication rules enabled for Cross-Region Replication.

**Identifier:** S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-default-lock-enabled

Checks if the S3 bucket has lock enabled, by default. The rule is NON_COMPLIANT if the lock is not enabled.

**Identifier:** S3_BUCKET_DEFAULT_LOCK_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

mode (Optional), Type: String

mode: (optional): A mode parameter with valid values of GOVERNANCE or COMPLIANCE.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-level-public-access-prohibited

Checks if S3 buckets are publicly accessible. The rule is NON_COMPLIANT if an S3 bucket is not listed in the `excludedPublicBuckets` parameter and bucket level settings are public.

**Identifier:** S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

excludedPublicBuckets (Optional), Type: CSV

Comma-separated list of known allowed public Amazon S3 bucket names.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-logging-enabled

Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled.

**Identifier:** S3_BUCKET_LOGGING_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

targetPrefix (Optional), Type: String

Prefix of the S3 bucket for storing server access logs.

targetBucket (Optional), Type: String

Target S3 bucket for storing server access logs.

### Proactive Evaluation

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "BucketName": "amzn-s3-demo-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "amzn-s3-demo-destination-bucket",
         "LogFilePrefix":"my-log"
   }
}
```

```
...
```

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-mfa-delete-enabled

Checks if MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled.

**Identifier:** S3_BUCKET_MFA_DELETE_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-policy-grantee-check

Checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or VPCs that you provide. The rule is COMPLIANT if a bucket policy is not present.

For example, if the input parameter to the rule is the list of two principals: 111122223333 and 444455556666 and the bucket policy specifies that only 111122223333 can access the bucket,

then the rule is COMPLIANT. With the same input parameters: If the bucket policy specifies that 111122223333 and 444455556666 can access the bucket, it is also COMPLIANT.

However, if the bucket policy specifies that 999900009999 can access the bucket, the rule is NON_COMPLIANT.

> **Note**
>
> If a bucket policy contains more than one statement, each statement in the bucket policy is evaluated against this rule.

**Identifier:** S3_BUCKET_POLICY_GRANTEE_CHECK

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

awsPrincipals (Optional), Type: CSV

Comma-separated list of principals such as IAM User ARNs, IAM Role ARNs, and AWS accounts. You must provide the full ARN or use partial matching. For example, "arn:aws:iam::*AccountID*:role/*role_name*" or "arn:aws:iam::*AccountID*:role/*". If the provided value is not an exact match with the principal ARN specified in the bucket policy, the rule is NON_COMPLIANT.

servicePrincipals (Optional), Type: CSV

Comma-separated list of service principals, for example 'cloudtrail.amazonaws.com, lambda.amazonaws.com'.

federatedUsers (Optional), Type: CSV

Comma-separated list of identity providers for web identity federation such as Amazon Cognito and SAML identity providers. For example 'cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider'.

ipAddresses (Optional), Type: CSV

Comma-separated list of CIDR formatted IP addresses, for example '10.0.0.1, 192.168.1.0/24, 2001:db8::/32'.

vpcIds (Optional), Type: CSV

Comma-separated list of Amazon Virtual Private Clouds (Amazon VPC) IDs, for example 'vpc-1234abc0, vpc-ab1234c0'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-policy-not-more-permissive

Checks if your Amazon Simple Storage Service bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide.

> **Note**
>
> If you provide an invalid parameter value, you will see the following error: Value for controlPolicy parameter must be an Amazon S3 bucket policy.

**Identifier:** S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

controlPolicy, Type: String

Amazon S3 bucket policy that defines an upper bound on the permissions of your S3 buckets. The policy can be a maximum of 1024 characters long.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-public-read-prohibited

Checks if your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

The rule is compliant when both of the following are true:

- The Block Public Access setting restricts public policies or the bucket policy does not allow public read access.
- The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public read access.

The rule is noncompliant when:

- If the Block Public Access setting does not restrict public policies, AWS Config evaluates whether the policy allows public read access. If the policy allows public read access, the rule is noncompliant.
- If the Block Public Access setting does not restrict public bucket ACLs, AWS Config evaluates whether the bucket ACL allows public read access. If the bucket ACL allows public read access, the rule is noncompliant.

> **Note**
>
> To be considered non-public, an S3 bucket policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

**Identifier:** S3_BUCKET_PUBLIC_READ_PROHIBITED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-public-write-prohibited

Checks if your Amazon S3 buckets do not allow public write access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

The rule is compliant when both of the following are true:

- The Block Public Access setting restricts public policies or the bucket policy does not allow public write access.
- The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public write access.

The rule is noncompliant when:

- If the Block Public Access setting does not restrict public policies, AWS Config evaluates whether the policy allows public write access. If the policy allows public write access, the rule is noncompliant.
- If the Block Public Access setting does not restrict public bucket ACLs, AWS Config evaluates whether the bucket ACL allows public write access. If the bucket ACL allows public write access, the rule is noncompliant.

> **Note**
>
> This rule does not evaluate changes to account level public block access. To check if the required public access block settings are configured from the account level, see s3-account-level-public-access-blocks and s3-account-level-public-access-blocks-periodic.

> **Note**
>
> To be considered non-public, an S3 bucket policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

**Identifier:** S3_BUCKET_PUBLIC_WRITE_PROHIBITED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-replication-enabled

Checks if S3 buckets have replication rules enabled. The rule is NON_COMPLIANT if an S3 bucket does not have a replication rule or has a replication rule that is not enabled.

**Identifier:** S3_BUCKET_REPLICATION_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

ReplicationType (Optional), Type: String

Accepted values: 'CROSS-REGION' and 'SAME-REGION'. Enter 'CROSS-REGION' for the rule to check that all buckets have only Cross-Region Replication enabled. Enter 'SAME-REGION' for the rule to check that all buckets have only Same-Region Replication enabled.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### s3-bucket-server-side-encryption-enabled

Checks if your Amazon S3 bucket either has the Amazon S3 default encryption enabled or that the Amazon S3 bucket policy explicitly denies `put-object` requests without server side encryption that uses AES-256 or AWS Key Management Service. The rule is NON_COMPLIANT if your Amazon S3 bucket is not encrypted by default.

**Identifier:** S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### s3-bucket-ssl-requests-only

Checks if S3 buckets have policies that require requests to use SSL/TLS. The rule is NON_COMPLIANT if any S3 bucket has policies allowing HTTP requests.

**Identifier:** S3_BUCKET_SSL_REQUESTS_ONLY

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-tagged

Checks if Amazon S3 buckets have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** S3_BUCKET_TAGGED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-bucket-versioning-enabled

Checks if versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets.

**Identifier:** S3_BUCKET_VERSIONING_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

isMfaDeleteEnabled (Optional), Type: String

MFA delete is enabled for your S3 buckets.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-default-encryption-kms

Checks if the S3 buckets are encrypted with AWS Key Management Service (AWS KMS). The rule is NON_COMPLIANT if the S3 bucket is not encrypted with an AWS KMS key.

**Identifier:** S3_DEFAULT_ENCRYPTION_KMS

**Resource Types:** AWS::S3::Bucket, AWS::KMS::Key

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma separated list of AWS KMS key ARNs allowed for encrypting Amazon S3 Buckets.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-event-notifications-enabled

Checks if Amazon S3 Events Notifications are enabled on an S3 bucket. The rule is NON_COMPLIANT if S3 Events Notifications are not set on a bucket, or if the event type or destination do not match the `eventTypes` and destinationArn parameters.

**Identifier:** S3_EVENT_NOTIFICATIONS_ENABLED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

destinationArn (Optional), Type: String

The Amazon Resource Name (ARN) of the destination for the event notification (Amazon SNS topic, AWS Lambda, Amazon SQS Queue).

eventTypes (Optional), Type: CSV

Comma-separated list of the preferred Amazon S3 event types

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-last-backup-recovery-point-created

Checks if a recovery point was created for Amazon Simple Storage Service (Amazon S3). The rule is NON_COMPLIANT if the Amazon S3 bucket does not have a corresponding recovery point created within the specified time period.

**Identifier:** S3_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon S3 bucket for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

Name of Amazon S3 bucket for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-lifecycle-policy-check

Checks if a lifecycle rule is configured for an Amazon Simple Storage Service (Amazon S3) bucket. The rule is NON_COMPLIANT if there is no active lifecycle configuration rules or the configuration does not match with the parameter values.

**Identifier:** S3_LIFECYCLE_POLICY_CHECK

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

targetTransitionDays (Optional), Type: int

Number of days after object creation when objects are transitioned to a specified storage class (for example, 30 days).

targetExpirationDays (Optional), Type: int

Number of days after object creation when objects are deleted (for example, 395 days).

targetTransitionStorageClass (Optional), Type: String

Destination storage class type. For example, Amazon S3 Standard-Infrequent Access (S3 Standard-IA). For more information, see Understanding and managing Amazon S3 storage classes.

targetPrefix (Optional), Type: String

Amazon S3 Object prefix to identify one or more objects.

bucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names that have lifecycle policy enabled.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-meets-restore-time-target

Checks if the restore time of Amazon Simple Storage Service (Amazon S3) buckets meets the specified duration. The rule is NON_COMPLIANT if LatestRestoreExecutionTimeMinutes of an Amazon S3 bucket is greater than maxRestoreTime minutes.

**Identifier:** S3_MEETS_RESTORE_TIME_TARGET

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

maxRestoreTime, Type: int

Numerical value for the maximum allowed restore runtime.

resourceTags (Optional), Type: String

Tags of Amazon S3 bucket for the rule to check, in JSON format.

resourceId (Optional), Type: String

Name of Amazon S3 bucket for the rule to check.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-resources-in-logically-air-gapped-vault

Checks if Amazon Simple Storage Service (Amazon S3) buckets are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon S3 bucket is not in a logically air-gapped vault within the specified time period.

**Identifier:** S3_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Periodic

**AWS Region:** Only available in Europe (Stockholm), Middle East (Bahrain), Asia Pacific (Mumbai), Europe (Paris), US East (Ohio), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Asia Pacific (Osaka), Europe (London), Asia Pacific (Tokyo), US West (Oregon), US West (N. California), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Amazon S3 bucket for the rule to check, in JSON format.

resourceId (Optional), Type: String

Name of Amazon S3 bucket for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 2184 for hours, 91 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-resources-protected-by-backup-plan

Checks if Amazon Simple Storage Service (Amazon S3) buckets are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon S3 bucket is not covered by a backup plan.

**Identifier:** S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for Amazon S3 buckets for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

Name of Amazon S3 bucket for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## s3-version-lifecycle-policy-check

Checks if Amazon Simple Storage Service (Amazon S3) version enabled buckets have lifecycle policy configured. The rule is NON_COMPLIANT if Amazon S3 lifecycle policy is not enabled.

**Identifier:** S3_VERSION_LIFECYCLE_POLICY_CHECK

**Resource Types:** AWS::S3::Bucket

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

bucketNames (Optional), Type: CSV

Comma-separated list of Amazon S3 bucket names that have lifecycle policy enabled.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-app-image-config-tagged

Checks if Amazon SageMaker app image configs have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** SAGEMAKER_APP_IMAGE_CONFIG_TAGGED

**Resource Types:** AWS::SageMaker::AppImageConfig

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS

GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-domain-in-vpc

Checks if an Amazon SageMaker domain uses a customer owned Amazon Virtual Private Cloud (VPC) for non-EFS traffic. The rule is NON_COMPLIANT if configuration.AppNetworkAccessType is not set to VpcOnly.

**Identifier:** SAGEMAKER_DOMAIN_IN_VPC

**Resource Types:** AWS::SageMaker::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-domain-tagged

Checks if Amazon SageMaker domains have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** SAGEMAKER_DOMAIN_TAGGED

**Resource Types:** AWS::SageMaker::Domain

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-endpoint-configuration-kms-key-configured

Checks if AWS Key Management Service (AWS KMS) key is configured for an Amazon SageMaker endpoint configuration. The rule is NON_COMPLIANT if 'KmsKeyId' is not specified for the Amazon SageMaker endpoint configuration.

**Identifier:** SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

**Resource Types:** AWS::SageMaker::EndpointConfig

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

kmsKeyArns (Optional), Type: String

Comma-separated list of specific AWS KMS key ARNs allowed for an Amazon SageMaker endpoint configuration.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-endpoint-config-prod-instance-count

Checks if Amazon SageMaker endpoint configurations have production variants `InitialInstanceCount` set to a value greater than 1. The rule is NON_COMPLIANT if production variants `InitialInstanceCount` is equal to 1.

**Identifier:** SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

**Resource Types:** AWS::SageMaker::EndpointConfig

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-feature-group-tagged

Checks if Amazon SageMaker feature groups have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** SAGEMAKER_FEATURE_GROUP_TAGGED

**Resource Types:** AWS::SageMaker::FeatureGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-image-description

Checks if Amazon SageMaker images have a description. The rule is NON_COMPLIANT if configuration.ImageDescription does not exist.

**Identifier:** SAGEMAKER_IMAGE_DESCRIPTION

**Resource Types:** AWS::SageMaker::Image

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-image-tagged

Checks if Amazon SageMaker images have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** SAGEMAKER_IMAGE_TAGGED

**Resource Types:** AWS::SageMaker::Image

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-model-in-vpc

Checks if an Amazon SageMaker model uses an Amazon Virtual Private Cloud (Amazon VPC) for container traffic. The rule is NON_COMPLIANT if configuration.VpcConfig does not exist.

**Identifier:** SAGEMAKER_MODEL_IN_VPC

**Resource Types:** AWS::SageMaker::Model

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-model-isolation-enabled

Checks if an Amazon SageMaker model has network isolation enabled. The rule is NON_COMPLIANT if configuration.EnableNetworkIsolation is false.

**Identifier:** SAGEMAKER_MODEL_ISOLATION_ENABLED

**Resource Types:** AWS::SageMaker::Model

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-notebook-instance-inside-vpc

Checks if an Amazon SageMaker notebook instance is launched within a VPC or within a list of approved subnets. The rule is NON_COMPLIANT if a notebook instance is not launched within a VPC or if its subnet ID is not included in the parameter list.

**Identifier:** SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

**Resource Types:** AWS::SageMaker::NotebookInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

SubnetIds (Optional), Type: CSV

Comma-separated list of subnet IDs that notebook instances can be launched in.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-notebook-instance-kms-key-configured

Checks if an AWS Key Management Service (AWS KMS) key is configured for an Amazon SageMaker notebook instance. The rule is NON_COMPLIANT if 'KmsKeyId' is not specified for the SageMaker notebook instance.

**Identifier:** SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

**Resource Types:** AWS::SageMaker::NotebookInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

kmsKeyArns (Optional), Type: String

Comma-separated list of AWS KMS key ARNs allowed for an Amazon SageMaker notebook instance.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-notebook-instance-platform-version

Checks if a Sagemaker Notebook Instance is configured to use a supported platform identifier version. The rule is NON_COMPLIANT if a Notebook Instance is not using the specified supported platform identifier version as specified in the parameter.

**Identifier:** SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

**Resource Types:** AWS::SageMaker::NotebookInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

supportedPlatformIdentifierVersions, Type: CSV

Comma-separated list of the supported platform identifier version for the rule to check.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-notebook-instance-root-access-check

Checks if the Amazon SageMaker RootAccess setting is enabled for Amazon SageMaker notebook instances. The rule is NON_COMPLIANT if the RootAccess setting is set to 'Enabled' for an Amazon SageMaker notebook instance.

**Identifier:** SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

**Resource Types:** AWS::SageMaker::NotebookInstance

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sagemaker-notebook-no-direct-internet-access

Checks if direct internet access is disabled for an Amazon SageMaker notebook instance. The rule is NON_COMPLIANT if a SageMaker notebook instance is internet-enabled.

**Identifier:** SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

**Resource Types:** AWS::SageMaker::NotebookInstance

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### secretsmanager-rotation-enabled-check

Checks if AWS Secrets Manager secret has rotation enabled. The rule also checks an optional `maximumAllowedRotationFrequency` parameter. If the parameter is specified, the rotation frequency of the secret is compared with the maximum allowed frequency. The rule is NON_COMPLIANT if the secret is not scheduled for rotation. The rule is also NON_COMPLIANT if the rotation frequency is higher than the number specified in the maximumAllowedRotationFrequency parameter.

> **Note**
>
> Re-evaluating this rule within 4 hours of the first evaluation will have no effect on the results.

**Identifier:** SECRETSMANAGER_ROTATION_ENABLED_CHECK

**Resource Types:** AWS::SecretsManager::Secret

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

maximumAllowedRotationFrequencyInHours (Optional), Type: int

Maximum allowed rotation frequency of the secret in hours.

maximumAllowedRotationFrequency (Optional), Type: int

Maximum allowed rotation frequency of the secret in days.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## secretsmanager-scheduled-rotation-success-check

Checks if AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated.

> **Note**
>
> **Recording delays**
> Evaluation results for this rule can be delayed for up to 2 days from a missed rotation date. For more immediate monitoring, see Monitor AWS Secrets Manager with Amazon CloudWatch in the *Secrets Manager User Guide*.
>
> **Secrets without rotation**
> The rule returns `NOT_APPLICABLE` for secrets that aren't configured for rotation.

**Identifier:** SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

**Resource Types:** AWS::SecretsManager::Secret

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## secretsmanager-secret-periodic-rotation

Checks if AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days.

**Identifier:** SECRETSMANAGER_SECRET_PERIODIC_ROTATION

**Resource Types:** AWS::SecretsManager::Secret

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

maxDaysSinceRotation (Optional), Type: int

Maximum number of days in which a secret can remain unchanged. The default value is 90 days.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## secretsmanager-secret-unused

Checks if AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days.

**Context**: It is recommended to routinely delete unused secrets. Unused secrets can be misused by former users who no longer need access to these secrets. Additionally, as more users gain access to a secret, it becomes increasingly possible that someone has misused a secret or has granted access to an unauthorized entity. Deleting unused secrets helps revoke secret access from users who no longer need it, and can reduce your cost of using AWS Secrets Manager.

**Identifier:** SECRETSMANAGER_SECRET_UNUSED

**Resource Types:** AWS::SecretsManager::Secret

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

unusedForDays (Optional), Type: int

The number of days in which a secret can remain unused. The default value is 90 days.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### secretsmanager-using-cmk

Checks if all secrets in AWS Secrets Manager are encrypted using the AWS managed key (`aws/secretsmanager`) or a customer managed key that was created in AWS Key Management Service (AWS KMS). The rule is COMPLIANT if a secret is encrypted using a customer managed key. This rule is NON_COMPLIANT if a secret is encrypted using `aws/secretsmanager`.

> **Note**
>
> This rule does not have access to cross-account customer managed keys and evaluates secrets as NON_COMPLIANT when a cross-account key is used.

**Identifier:** SECRETSMANAGER_USING_CMK

**Resource Types:** AWS::SecretsManager::Secret

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

kmsKeyArns (Optional), Type: CSV

Comma-separated list of KMS key Amazon Resource Names (ARNs) to check if the keys are used in the encryption.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### securityhub-enabled

Checks if AWS Security Hub is enabled for an AWS Account. The rule is NON_COMPLIANT if AWS Security Hub is not enabled.

**Identifier:** SECURITYHUB_ENABLED

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### security-account-information-provided

Checks if you have provided security contact information for your AWS account contacts. The rule is NON_COMPLIANT if security contact information within the account is not provided.

**Identifier:** SECURITY_ACCOUNT_INFORMATION_PROVIDED

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## service-catalog-portfolio-tagged

Checks if AWS Service Catalog portfolio resources have tags. Optionally, required tag keys can be specified. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** SERVICE_CATALOG_PORTFOLIO_TAGGED

**Resource Types:** AWS::ServiceCatalog::Portfolio

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## service-catalog-shared-within-organization

Checks if AWS Service Catalog shares portfolios to an organization (a collection of AWS accounts treated as a single unit) when integration is enabled with AWS Organizations. The rule is NON_COMPLIANT if the `Type` value of a share is `ACCOUNT`.

**Identifier:** SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

**Resource Types:** AWS::ServiceCatalog::Portfolio

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## service-vpc-endpoint-enabled

Checks if Service Endpoint for the service provided in rule parameter is created for each Amazon Virtual Private Cloud (Amazon VPC). The rule is NON_COMPLIANT if an Amazon VPC doesn't have an Amazon VPC endpoint created for the service.

**Identifier:** SERVICE_VPC_ENDPOINT_ENABLED

**Resource Types:** AWS::EC2::VPC

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

serviceName, Type: String

The short name or suffix for the service. Note: To get a list of available service names or valid suffix list, use DescribeVpcEndpointServices.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ses-malware-scanning-enabled

Checks if malware and spam scanning on receiving messages is enabled for Amazon Simple Email Service (Amazon SES). The rule is NON_COMPLIANT if malware and spam scanning is not enabled.

**Identifier:** SES_MALWARE_SCANNING_ENABLED

**Resource Types:** AWS::SES::ReceiptRule

**Trigger type:** Periodic

**AWS Region:** Only available in Europe (Ireland), US East (N. Virginia), US West (Oregon) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ses-sending-tls-required

Checks if Amazon Simple Email Service (SES) Configuration Set has TLS encryption enforced for email delivery. The rule is NON_COMPLIANT if the TLS Policy is not set to 'REQUIRE' in the Configuration Set.

**Identifier:** SES_SENDING_TLS_REQUIRED

**Resource Types:** AWS::SES::ConfigurationSet

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Middle East (UAE), Asia Pacific (Hong Kong), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## shield-advanced-enabled-autorenew

Checks if AWS Shield Advanced is enabled in your AWS account and this subscription is set to automatically renew. The rule is COMPLIANT if Shield Advanced is enabled and auto renew is enabled.

> **Note**
>
> The API endpoint of AWS Shield Advanced is only available in US East (N. Virginia) Region. This rule should only be scheduled to run in the US East (N. Virginia) Region.

**Identifier:** SHIELD_ADVANCED_ENABLED_AUTORENEW

**Trigger type:** Periodic

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## shield-drt-access

Checks if the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured.

**Identifier:** SHIELD_DRT_ACCESS

**Trigger type:** Periodic

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sns-encrypted-kms

Checks if SNS topics are encrypted with AWS Key Management Service (AWS KMS). The rule is NON_COMPLIANT if an SNS topic is not encrypted with AWS KMS. Optionally, specify the key ARNs, the alias ARNs, the alias name, or the key IDs for the rule to check.

**Identifier:** SNS_ENCRYPTED_KMS

**Resource Types:** AWS::SNS::Topic

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

kmsKeyIds (Optional), Type: CSV

Comma-separated list of AWS KMS key Amazon Resource Names (ARNs), KMS alias ARNs, KMS alias names, or KMS key IDs for the rule to check.

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sns-topic-message-delivery-notification-enabled

Checks if Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled.

**Identifier:** SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

**Resource Types:** AWS::SNS::Topic

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS

GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sns-topic-no-public-access

Checks if the SNS topic access policy allows public access. The rule is NON_COMPLIANT if the SNS topic access policy allows public access.

> **Note**
>
> To be considered non-public, an SNS policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

**Identifier:** SNS_TOPIC_NO_PUBLIC_ACCESS

**Resource Types:** AWS::SNS::Topic

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sqs-queue-dlq-check

Checks if Amazon Simple Queue Service (Amazon SQS) queues have configuration to use dead-letter queue (DLQ). The rule is NON_COMPLIANT if an Amazon SQS queue does not have any configuration to use DLQ.

**Identifier:** SQS_QUEUE_DLQ_CHECK

**Resource Types:** AWS::SQS::Queue

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sqs-queue-no-public-access

Checks if the SQS queue access policy allows public access. The rule is NON_COMPLIANT if the SQS queue access policy allows public access.

> **Note**
>
> To be considered non-public, an SQS policy must grant access only to fixed values. This means values that don't contain a wildcard or the following IAM policy element: Variables.

**Identifier:** SQS_QUEUE_NO_PUBLIC_ACCESS

**Resource Types:** AWS::SQS::Queue

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## sqs-queue-policy-full-access-check

Checks if the SQS queue access policy allows full access. The rule is NON_COMPLIANT if the SQS policy contains `SQS:*` within `Action` and `Effect` is `Allow`.

**Identifier:** SQS_QUEUE_POLICY_FULL_ACCESS_CHECK

**Resource Types:** AWS::SQS::Queue

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ssm-automation-block-public-sharing

Checks if AWS Systems Manager Documents has block public sharing enabled. The rule is NON_COMPLIANT if Systems Manager Documents has block public sharing disabled.

**Identifier:** SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ssm-automation-logging-enabled

Checks if AWS Systems Manager Automation has Amazon CloudWatch logging enabled. The rule returns NON_COMPLIANT if Systems Manager Automation doesn't have CloudWatch logging enabled.

**Identifier:** SSM_AUTOMATION_LOGGING_ENABLED

**Resource Types:** AWS::::Account

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ssm-document-not-public

Checks if AWS Systems Manager documents owned by the account are public. The rule is NON_COMPLIANT if Systems Manager documents with the owner 'Self' are public.

**Identifier:** SSM_DOCUMENT_NOT_PUBLIC

**Resource Types:** AWS::SSM::Document

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Taipei) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## ssm-document-tagged

Checks if AWS Systems Manager documents have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** SSM_DOCUMENT_TAGGED

**Resource Types:** AWS::SSM::Document

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## stepfunctions-state-machine-tagged

Checks if AWS Step Functions state machines have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** STEPFUNCTIONS_STATE_MACHINE_TAGGED

**Resource Types:** AWS::StepFunctions::StateMachine

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## step-functions-state-machine-logging-enabled

Checks if AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided.

**Identifier:** STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

**Resource Types:** AWS::StepFunctions::StateMachine

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

cloudWatchLogGroupArns (Optional), Type: CSV

Comma-separated list of Amazon Resource Names (ARNs) for Amazon CloudWatch Logs log groups. The rule checks if the specified log groups are configured for your state machine logs.

logLevel (Optional), Type: String

The minimum log level for your state machine. Valid values include: ALL, ERROR, FATAL.

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## storagegateway-last-backup-recovery-point-created

Checks if a recovery point was created for AWS Storage Gateway volumes. The rule is NON_COMPLIANT if the Storage Gateway volume does not have a corresponding recovery point created within the specified time period.

**Identifier:** STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::StorageGateway::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Storage Gateway volumes for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of Storage Gateway volume for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## storagegateway-resources-in-logically-air-gapped-vault

Checks if AWS Storage Gateway volumes are in a logically air-gapped vault. The rule is NON_COMPLIANT if an AWS Storage Gateway volume is not in a logically air-gapped vault within the specified time period.

**Identifier:** STORAGEGATEWAY_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

**Resource Types:** AWS::StorageGateway::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of Storage Gateway volumes for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Storage Gateway volume for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 2184 for hours, 91 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## storagegateway-resources-protected-by-backup-plan

Checks if AWS Storage Gateway volumes are protected by a backup plan. The rule is NON_COMPLIANT if the Storage Gateway volume is not covered by a backup plan.

**Identifier:** STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::StorageGateway::Volume

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for Storage Gateway Volumes for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of Storage Gateway volume for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## subnet-auto-assign-public-ip-disabled

Checks if Amazon Virtual Private Cloud (Amazon VPC) subnets are assigned a public IP address. The rule is COMPLIANT if Amazon VPC does not have subnets that are assigned a public IP address. The rule is NON_COMPLIANT if Amazon VPC has subnets that are assigned a public IP address.

**Identifier:** SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

**Resource Types:** AWS::EC2::Subnet

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions

**Parameters:**

None

**Proactive Evaluation**

For steps on how to run this rule in proactive mode, see Evaluating Your Resources with AWS Config Rules. For this rule to return COMPLIANT in proactive mode, the resource configuration schema for the StartResourceEvaluation API needs to include the following inputs, encoded as a string:

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

For more information on proactive evaluation, see Evaluation Mode.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-agreement-description

Checks if AWS Transfer Family agreements have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** TRANSFER_AGREEMENT_DESCRIPTION

**Resource Types:** AWS::Transfer::Agreement

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-agreement-tagged

Checks if AWS Transfer Family agreements have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** TRANSFER_AGREEMENT_TAGGED

**Resource Types:** AWS::Transfer::Agreement

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-certificate-description

Checks if AWS Transfer Family certificates have a description. The rule is NON_COMPLIANT if configuration.Description does not exist.

**Identifier:** TRANSFER_CERTIFICATE_DESCRIPTION

**Resource Types:** AWS::Transfer::Certificate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-certificate-tagged

Checks if AWS Transfer Family certificates have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** TRANSFER_CERTIFICATE_TAGGED

**Resource Types:** AWS::Transfer::Certificate

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-connector-logging-enabled

Checks if AWS Transfer Family Connector publishes logs to Amazon CloudWatch. The rule is NON_COMPLIANT if a Connector does not have a LoggingRole assigned.

**Identifier:** TRANSFER_CONNECTOR_LOGGING_ENABLED

**Resource Types:** AWS::Transfer::Connector

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), Asia Pacific (Thailand), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-connector-tagged

Checks if AWS Transfer Family connectors have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** TRANSFER_CONNECTOR_TAGGED

**Resource Types:** AWS::Transfer::Connector

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-family-server-no-ftp

Checks if a server created with AWS Transfer Family uses FTP for endpoint connection. The rule is NON_COMPLIANT if the server protocol for endpoint connection is FTP-enabled.

**Identifier:** TRANSFER_FAMILY_SERVER_NO_FTP

**Resource Types:** AWS::Transfer::Server

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-profile-tagged

Checks if AWS Transfer Family profiles have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** TRANSFER_PROFILE_TAGGED

**Resource Types:** AWS::Transfer::Profile

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

> Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-workflow-description

Checks if AWS Transfer Family workflows have a description. The rule is NON_COMPLIANT if configuration.Description does not exist or is an empty string.

**Identifier:** TRANSFER_WORKFLOW_DESCRIPTION

**Resource Types:** AWS::Transfer::Workflow

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## transfer-workflow-tagged

Checks if AWS Transfer Family workflows have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** TRANSFER_WORKFLOW_TAGGED

**Resource Types:** AWS::Transfer::Workflow

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## virtualmachine-last-backup-recovery-point-created

Checks if a recovery point was created for AWS Backup-Gateway VirtualMachines. The rule is NON_COMPLIANT if an AWS Backup-Gateway VirtualMachines does not have a corresponding recovery point created within the specified time period.

**Identifier:** VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

**Resource Types:** AWS::BackupGateway::VirtualMachine

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of AWS Backup-Gateway VirtualMachines for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of AWS Backup-Gateway VirtualMachine for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 744 for hours, 31 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## virtualmachine-resources-in-logically-air-gapped-vault

Checks if AWS Backup-Gateway VirtualMachines are in a logically air-gapped vault. The rule is NON_COMPLIANT if an AWS Backup-Gateway VirtualMachines is not in a logically air-gapped vault within the specified time period.

**Identifier:** VIRTUALMACHINE_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

**Resource Types:** AWS::BackupGateway::VirtualMachine

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags of AWS Backup-Gateway VirtualMachines for the rule to check, in JSON format.

resourceId (Optional), Type: String

ID of AWS Backup-Gateway VirtualMachine for the rule to check.

recoveryPointAgeValue (Optional), Type: int, Default: 1

Numerical value for maximum allowed age. No more than 2184 for hours, 91 for days.

recoveryPointAgeUnit (Optional), Type: String, Default: days

Unit of time for maximum allowed age. Accepted values: 'hours', 'days'.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## virtualmachine-resources-protected-by-backup-plan

Checks if AWS Backup-Gateway VirtualMachines are protected by a backup plan. The rule is NON_COMPLIANT if the Backup-Gateway VirtualMachine is not covered by a backup plan.

**Identifier:** VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

**Resource Types:** AWS::BackupGateway::VirtualMachine

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

resourceTags (Optional), Type: String

Tags for AWS Backup-Gateway VirtualMachines for the rule to check, in JSON format `{"tagkey" : "tagValue"}`.

resourceId (Optional), Type: String

ID of AWS Backup-Gateway VirtualMachine for the rule to check.

crossRegionList (Optional), Type: String

Comma-separated list of destination regions for the cross-region backup copy to be kept

crossAccountList (Optional), Type: String

Comma-separated list of destination accounts for cross-account backup copy to be kept

maxRetentionDays (Optional), Type: int

The maximum retention period in days for the Backup Vault Lock

minRetentionDays (Optional), Type: int

The minimum retention period in days for the Backup Vault Lock

backupVaultLockCheck (Optional), Type: String

Accepted values: 'True' or 'False'. Enter 'True' for the rule to check if the resource is backed up in a locked vault

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## vpc-default-security-group-closed

Checks if the default security group of any Amazon Virtual Private Cloud (Amazon VPC) does not allow inbound or outbound traffic. The rule is NON_COMPLIANT if the default security group has one or more inbound or outbound traffic rules.

> **Note**
>
> There may be a delay between when AWS Config records the deletion of related resources such as default security groups, which are deleted as part of the Amazon VPC deletion. As a result, even if all default security groups or other related resources have been deleted or remediated, the rule may report NON_COMPLIANT until the next account baselining process.

**Identifier:** VPC_DEFAULT_SECURITY_GROUP_CLOSED

**Resource Types:** AWS::EC2::SecurityGroup

**Trigger type:** Configuration changes

**AWS Region:** Only available in Middle East (Bahrain), US East (Ohio), Europe (Ireland), Europe (Frankfurt), US East (N. Virginia), US West (Oregon) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## vpc-endpoint-enabled

Checks if each service specified in the parameter has an Amazon VPC endpoint. The rule is NON_COMPLIANT if Amazon VPC does not have a VPC endpoint created for each specified service. Optionally, you can specify certain VPCs for the rule to check.

**Identifier:** VPC_ENDPOINT_ENABLED

**Resource Types:** AWS::EC2::VPC

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Osaka), Asia Pacific (Malaysia), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

serviceNames, Type: CSV

Comma-separated list of service names or endpoints. Example: "access-analyzer, appconfig, cloudtrail" or "com.amazonaws.region.access-analyzer". Use DescribeVpcEndpointServices for available names.

vpcIds (Optional), Type: CSV

Comma-separated list of Amazon VPC IDs for VPC endpoints. If provided, the rule is NON_COMPLIANT if the services specified in the serviceName parameter do not have one of these VPC endpoints.

scopeConfigResourceTypes (Optional), Type: CSV

Comma-separated list of AWS Config resource types for the rule to check. If specified, the rule returns a compliance status only if at least one specified resource is recorded in the account. For example: "AWS::SNS::Topic".

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## vpc-flow-logs-enabled

Checks if Amazon Virtual Private Cloud (Amazon VPC) flow logs are found and enabled for all Amazon VPCs. The rule is NON_COMPLIANT if flow logs are not enabled for at least one Amazon VPC.

**Identifier:** VPC_FLOW_LOGS_ENABLED

**Resource Types:** AWS::EC2::VPC

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

trafficType (Optional), Type: String

TrafficType of flow logs

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## vpc-network-acl-unused-check

Checks if there are unused network access control lists (network ACLs). The rule is COMPLIANT if each network ACL is associated with a subnet. The rule is NON_COMPLIANT if a network ACL is not associated with a subnet.

**Identifier:** VPC_NETWORK_ACL_UNUSED_CHECK

**Resource Types:** AWS::EC2::NetworkAcl

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## vpc-peering-dns-resolution-check

Checks if DNS resolution from accepter/requester VPC to private IP is enabled. The rule is NON_COMPLIANT if DNS resolution from accepter/requester VPC to private IP is not enabled.

**Identifier:** VPC_PEERING_DNS_RESOLUTION_CHECK

**Resource Types:** AWS::EC2::VPCPeeringConnection

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

vpcIds (Optional), Type: CSV

Comma-separated list of VPC IDs to be checked.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## vpc-sg-open-only-to-authorized-ports

Checks if security groups allowing unrestricted incoming traffic ('0.0.0.0/0' or '::/0') only allow inbound TCP or UDP connections on authorized ports. The rule is NON_COMPLIANT if such security groups do not have ports specified in the rule parameters.

> **Note**
>
> This rule evaluates Amazon EC2 security groups with ingress rule set to IPv4='0.0.0.0/0' or IPv6='::/'. If the security group does not have one of those destinations, this rule returns `NOT_APPLICABLE`.

**Identifier:** VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

**Resource Types:** AWS::EC2::SecurityGroup

**Trigger type:** Configuration changes and Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

authorizedTcpPorts (Optional), Type: String

Comma-separated list of TCP ports authorized to be open to 0.0.0.0/0 or ::/0. Ranges are defined by dash, for example, "443,1020-1025".

authorizedUdpPorts (Optional), Type: String

Comma-separated list of UDP ports authorized to be open to 0.0.0.0/0 or ::/0. Ranges are defined by dash, for example, "500,1020-1025".

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## vpc-sg-port-restriction-check

Checks if security groups restrict incoming traffic to restricted ports explicitly from 0.0.0.0/0 or ::/0. The rule is NON_COMPLIANT if security groups allow incoming traffic from 0.0.0.0/0 or ::/0 over TCP/UDP ports 22/3389 or as specified in parameters.

**Identifier:** VPC_SG_PORT_RESTRICTION_CHECK

**Resource Types:** AWS::EC2::SecurityGroup

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Malaysia), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

restrictPorts (Optional), Type: CSV

Comma-separated list of ports that should not be open for incoming traffic over the full IP range. Valid port numbers range from 0 to 65535. If not specified, the rule defaults to check for 22 and 3389.

protocolType (Optional), Type: String

The Transmission Protocol Type for the rule to check. Valid values include 'TCP', 'UDP', and 'ALL' (case-insensitive). If set to 'ALL', the rule will check for rules that use either 'TCP', 'UDP', or 'ALL' (-1) protocol. Default value is 'ALL'.

excludeExternalSecurityGroups (Optional), Type: boolean

Boolean flag to exclude the evaluation of external security groups. If set to 'true', the rule will not include external security groups in the evaluation. Otherwise, all security groups are evaluated if value is set to 'false.' Default value is 'true'.

ipType (Optional), Type: String

The Internet Protocol (IP) version for the rule to check. Valid values include 'IPv4', 'IPv6', and 'ALL' (case-insensitive). If not specified, the rule defaults to check for 'ALL'.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### vpc-vpn-2-tunnels-up

Checks if both virtual private network (VPN) tunnels provided by AWS Site-to-Site VPN are in UP status. The rule is NON_COMPLIANT if one or both tunnels are in DOWN status.

**Identifier:** VPC_VPN_2_TUNNELS_UP

**Resource Types:** AWS::EC2::VPNConnection

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Middle East (Bahrain), China (Beijing), Asia Pacific (Osaka), Israel (Tel Aviv), China (Ningxia) Region

**Parameters:**

None

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

### wafv2-logging-enabled

Checks if logging is enabled on AWS WAFv2 regional and global web access control lists (web ACLs). The rule is NON_COMPLIANT if the logging is enabled but the logging destination does not match the value of the parameter.

> **Note**
>
> **Amazon Security Lake Exception**
> This rule does not check logging done with Security Lake for AWS WAFV2 web ACLs.

**Identifier:** WAFV2_LOGGING_ENABLED

**Resource Types:** AWS::WAFv2::WebACL

**Trigger type:** Periodic

**AWS Region:** All supported AWS regions

**Parameters:**

KinesisFirehoseDeliveryStreamArns (Optional), Type: CSV

Comma separated list of Kinesis Firehose delivery stream ARNs

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## wafv2-rulegroup-logging-enabled

Checks if Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false.

**Context**: AWS WAFV2 (Web Application Firewall version 2) allows you to create AWS WAF rules to protect your web applications from common web exploits and vulnerabilities. An AWS WAF rule group is a collection of AWS WAF rules that you can associate with a web ACL (Access Control List) to define the desired behavior for your web application traffic. For more information, see AWS WAF rules and Rule groups in the *AWS WAF Developer Guide*.

By configuring CloudWatch security metrics collection on AWS WAFV2 rules group, you can monitor security metrics such as successful or failed Distributed denial of service (DDoS), SQL injection, and Cross-site scripting (XSS) attacks. The security metrics collected can help you simplify your investigations.

> **Note**
>
> If there are no AWS WAF rules in the AWS WAFV2 rule group for the AWS Config managed rule to check, the AWS Config managed rule returns `NOT_APPLICABLE`.

**Identifier:** WAFV2_RULEGROUP_LOGGING_ENABLED

**Resource Types:** AWS::WAFv2::RuleGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## wafv2-rulegroup-not-empty

Checks if WAFv2 Rule Groups contain rules. The rule is NON_COMPLIANT if there are no rules in a WAFv2 Rule Group.

**Identifier:** WAFV2_RULEGROUP_NOT_EMPTY

**Resource Types:** AWS::WAFv2::RuleGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), Asia Pacific (Melbourne), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## wafv2-webacl-not-empty

Checks if a WAFv2 Web ACL contains any WAF rules or WAF rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rules or WAF rule groups.

**Identifier:** WAFV2_WEBACL_NOT_EMPTY

**Resource Types:** AWS::WAFv2::WebACL

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), Europe (Zurich) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## waf-classic-logging-enabled

Checks if logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled.

**Identifier:** WAF_CLASSIC_LOGGING_ENABLED

**Resource Types:** AWS::WAF::WebACL

**Trigger type:** Periodic

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

KinesisFirehoseDeliveryStreamArns (Optional), Type: CSV

Comma separated list of Amazon Kinesis stream ARN for AWS WAF logs.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## waf-global-rulegroup-not-empty

Checks if an AWS WAF Classic rule group contains any rules. The rule is NON_COMPLIANT if there are no rules present within a rule group.

**Identifier:** WAF_GLOBAL_RULEGROUP_NOT_EMPTY

**Resource Types:** AWS::WAF::RuleGroup

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## waf-global-rule-not-empty

Checks if an AWS WAF global rule contains any conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule.

**Identifier:** WAF_GLOBAL_RULE_NOT_EMPTY

**Resource Types:** AWS::WAF::Rule

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## waf-global-webacl-not-empty

Checks whether a WAF Global Web ACL contains any WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group.

**Identifier:** WAF_GLOBAL_WEBACL_NOT_EMPTY

**Resource Types:** AWS::WAF::WebACL

**Trigger type:** Configuration changes

**AWS Region:** Only available in US East (N. Virginia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## waf-regional-rulegroup-not-empty

Checks if WAF Regional rule groups contain any rules. The rule is NON_COMPLIANT if there are no rules present within a WAF Regional rule group.

**Identifier:** WAF_REGIONAL_RULEGROUP_NOT_EMPTY

**Resource Types:** AWS::WAFRegional::RuleGroup

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except China (Beijing), Asia Pacific (Thailand), Asia Pacific (Jakarta), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Israel (Tel Aviv), Asia Pacific (Taipei), Canada West (Calgary), Europe (Spain), China (Ningxia), Europe (Zurich) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## waf-regional-rule-not-empty

Checks whether WAF regional rule contains conditions. This rule is COMPLIANT if the regional rule contains at least one condition and NON_COMPLIANT otherwise.

**Identifier:** WAF_REGIONAL_RULE_NOT_EMPTY

**Resource Types:** AWS::WAFRegional::Rule

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## waf-regional-webacl-not-empty

Checks if a WAF regional Web ACL contains any WAF rules or rule groups. The rule is NON_COMPLIANT if there are no WAF rules or rule groups present within a Web ACL.

**Identifier:** WAF_REGIONAL_WEBACL_NOT_EMPTY

**Resource Types:** AWS::WAFRegional::WebACL

**Trigger type:** Configuration changes

**AWS Region:** All supported AWS regions except Asia Pacific (Thailand), Asia Pacific (Malaysia), AWS GovCloud (US-East), AWS GovCloud (US-West), Mexico (Central), Asia Pacific (Taipei), Canada West (Calgary) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## workspaces-connection-alias-tagged

Checks if Amazon WorkSpaces connection aliases have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** WORKSPACES_CONNECTION_ALIAS_TAGGED

**Resource Types:** AWS::WorkSpaces::ConnectionAlias

**Trigger type:** Configuration changes

**AWS Region:** Only available in Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## workspaces-root-volume-encryption-enabled

Checks if an Amazon WorkSpace volume has the root volume encryption settings set to enabled. This rule is NON_COMPLIANT if the encryption setting is not enabled for the root volume.

**Identifier:** WORKSPACES_ROOT_VOLUME_ENCRYPTION_ENABLED

**Resource Types:** AWS::WorkSpaces::Workspace

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Africa (Cape Town), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central), China (Ningxia) Region

**Parameters:**

None

**AWS CloudFormation template**

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## workspaces-user-volume-encryption-enabled

Checks if an Amazon WorkSpace volume has the user volume encryption settings set to enabled. This rule is NON_COMPLIANT if the encryption setting is not enabled for the user volume.

**Identifier:** WORKSPACES_USER_VOLUME_ENCRYPTION_ENABLED

**Resource Types:** AWS::WorkSpaces::Workspace

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Africa (Cape Town), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central), China (Ningxia) Region

**Parameters:**

None

### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## workspaces-workspace-tagged

Checks if Amazon WorkSpaces workspaces have tags. Optionally, you can specify tag keys. The rule is NON_COMPLIANT if there are no tags or if the specified tag keys are not present. The rule does not check for tags starting with 'aws:'.

**Identifier:** WORKSPACES_WORKSPACE_TAGGED

**Resource Types:** AWS::WorkSpaces::Workspace

**Trigger type:** Configuration changes

**AWS Region:** Only available in Asia Pacific (Mumbai), Africa (Cape Town), Europe (Ireland), Europe (Frankfurt), South America (Sao Paulo), US East (N. Virginia), Asia Pacific (Seoul), Europe (London), Asia Pacific (Tokyo), US West (Oregon), Asia Pacific (Singapore), Asia Pacific (Sydney), Canada (Central) Region

**Parameters:**

requiredKeyTags (Optional), Type: CSV

Comma-separated list of tag keys for the rule to check. If provided, the rule is NON_COMPLIANT if the evaluated resource does not contain these keys. Tag keys are case-sensitive. Tag keys starting with 'aws:' are not allowed.

#### AWS CloudFormation template

To create AWS Config managed rules with AWS CloudFormation templates, see Creating AWS Config Managed Rules With AWS CloudFormation Templates.

## List of AWS Config Managed Rules by Evaluation Mode

AWS Config currently supports the following managed rules. Before using these rules, see Considerations.

### Proactive Evaluation

*Proactive rules* are rules that support the proactive evaluation mode for resources that have not been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region. For more information, see Evaluation modes.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

#### Proactive Evaluation

- eip-attached

### Detective Evaluation

*Detective rules* are rules that support the detective evaluation mode for resource that have already been deployed. This allows you to evaluate the configuration settings of your existing resources.

> **Note**
>
> Currently, all AWS Config rules support detective evaluation.

### Detective Evaluation

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled

- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged

- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-distribution-key-group-enabled
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-oac-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https

- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled

- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured

- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required

- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged

- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion

- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged

- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled

- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check

- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-health-check-tagged
- route53-hosted-zone-tagged
- route53-query-logging-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled

- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## List of AWS Config Managed Rules by Trigger Type

AWS Config currently supports the following managed rules. Before using these rules, see Considerations.

### Configuration Changes

*Change-triggered rules* are rules that AWS Config evaluates in response to configuration changes.

#### Configuration Changes

- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description

- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage

- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check

- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-distribution-key-group-enabled
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-oac-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check
- cloudwatch-metric-stream-tagged
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged

- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance

- ebs-snapshot-block-public-access
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check

- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- eks-fargate-profile-tagged
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged

- glue-spark-job-supported-version
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-saml-provider-tagged
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged

- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged

- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled

- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-tagged
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-health-check-tagged
- route53-hosted-zone-tagged
- route53-query-logging-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged

- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged

- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Periodic

*Periodic rules* are rules that AWS Config evaluates periodicially at a frequency that you specify; for example, every 24 hours.

### Periodic

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf

- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-encryption-enabled
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-server-certificate-expiration-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled
- nlb-logging-enabled
- rds-instance-subnet-igw-check
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-mysql-instance-encrypted-in-transit
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-sqlserver-encrypted-in-transit
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- waf-classic-logging-enabled

## Hybrid

*Hybrid rules* are rules that AWS Config evaluates both in response to configuration changes and periodicially.

### Hybrid

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- ec2-instance-launched-with-allowed-ami

- incoming-ssh-disabled
- no-unrestricted-route-to-igw
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

## List of AWS Config Managed Rules by Region Availability

AWS Config currently supports the following managed rules. Before using these rules, see Considerations.

### US East (Ohio) Region

#### US East (Ohio)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description

- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled

- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check

- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami

- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged

- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit

- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled

- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit

- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access

- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp

- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## US East (N. Virginia) Region

### US East (N. Virginia)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled

- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target

- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-distribution-key-group-enabled
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-oac-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled

- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled

- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled

- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted

- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged

- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check

- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- route53-health-check-tagged
- route53-hosted-zone-tagged
- route53-query-logging-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## US West (N. California) Region

### US West (N. California)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged

- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check

- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check

- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging

- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user

- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized

- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description

- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check

- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## US West (Oregon) Region

### US West (Oregon)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled

- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target

- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled

- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists

- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access

- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check

- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged

- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Africa (Cape Town) Region

### Africa (Cape Town)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged

- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged

- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged

- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged

- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled

- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Asia Pacific (Hong Kong) Region

### Asia Pacific (Hong Kong)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged

- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled

- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check

- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged

- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged

- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check

- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Asia Pacific (Hyderabad) Region

### Asia Pacific (Hyderabad)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public

- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled

- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled

- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Asia Pacific (Jakarta) Region

### Asia Pacific (Jakarta)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged

- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged

- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created

- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check

- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged

- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled

- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Asia Pacific (Malaysia) Region

### Asia Pacific (Malaysia)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-redirection-check
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- beanstalk-enhanced-health-reporting-enabled

- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-logging-enabled

- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public

- subnet-auto-assign-public-ip-disabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## Asia Pacific (Melbourne) Region

### Asia Pacific (Melbourne)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged

- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- approved-amis-by-id
- approved-amis-by-tag
- appsync-graphql-api-xray-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault

- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan

- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check

- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled

- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan

- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Asia Pacific (Mumbai) Region

### Asia Pacific (Mumbai)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled

- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged

- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption

- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled

- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled

- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target

- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check

- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged

- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs

- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest

- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check

- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check

- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Asia Pacific (Osaka) Region

### Asia Pacific (Osaka)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description

- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled

- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled

- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit

- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged

- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled

- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled

- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check

- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Asia Pacific (Seoul) Region

### Asia Pacific (Seoul)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description

- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged

- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled

- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check

- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled

- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled

- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch

- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Asia Pacific (Singapore) Region

### Asia Pacific (Singapore)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check

- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest

- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest

- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled

- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists

- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch

- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged

- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Asia Pacific (Sydney) Region

### Asia Pacific (Sydney)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description

- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged

- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault

- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check

- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check

- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check

- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required

- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged

- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit

- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Asia Pacific (Taipei) Region

### Asia Pacific (Taipei)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-redirection-check
- approved-amis-by-id
- approved-amis-by-tag
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## Asia Pacific (Thailand) Region

### Asia Pacific (Thailand)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-redirection-check
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag

- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited

- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-level-public-access-prohibited
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## Asia Pacific (Tokyo) Region

### Asia Pacific (Tokyo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged

- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description

- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled

- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check

- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check

- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled

- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni

- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled

- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled

- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled

- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged

- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged

- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Canada (Central) Region

### Canada (Central)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description

- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged

- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration

- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged

- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled

- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged

- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled

- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled

- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged

- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Canada West (Calgary) Region

### Canada West (Calgary)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged

- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- aurora-mysql-cluster-audit-logging
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- cw-loggroup-retention-period-check

- datasync-task-data-verification-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-prefix-list-tagged
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-tagged
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-encrypted-check
- efs-file-system-tagged
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- glb-tagged
- glue-ml-transform-tagged
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- multi-region-cloud-trail-enabled

- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## China (Beijing) Region

### China (Beijing)

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id

- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-logging
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami

- ec2-instance-managed-by-ssm
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-function-public-access-prohibited
- lambda-function-xray-enabled
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled

- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-enhanced-monitoring-enabled
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check

- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-routes-within-vpc
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## China (Ningxia) Region

### China (Ningxia)

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-logging
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging

- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check

- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-capacity-provider-termination-check

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc

- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- netfw-subnet-change-protection-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest

- rds-enhanced-monitoring-enabled
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-routes-within-vpc
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check

- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

## Europe (Frankfurt) Region

### Europe (Frankfurt)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault

- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled

- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check

- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged

- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit

- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Europe (Ireland) Region

### Europe (Ireland)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc

- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check

- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair

- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged

- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled

- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled

- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created

- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Europe (London) Region

### Europe (London)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id

- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check

- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan

- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged

- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check

- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged

- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc

- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## Europe (Milan) Region

### Europe (Milan)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled

- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled

- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached

- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit

- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled

- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check

- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms

- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Europe (Paris) Region

### Europe (Paris)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled

- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-type-check
- apprunner-service-max-unhealthy-threshold
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created

- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description

- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists

- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled

- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check

- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version

- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description

- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Europe (Spain) Region

### Europe (Spain)

- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check

- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged

- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance

- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest

- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check

- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Europe (Stockholm) Region

### Europe (Stockholm)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged

- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged

- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled

- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni

- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-allow-public-overrides-disabled
- lightsail-bucket-tagged

- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication

- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged

- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan

- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access

- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Europe (Zurich) Region

### Europe (Zurich)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached

- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest

- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created

- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check

- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Israel (Tel Aviv) Region

### Israel (Tel Aviv)

- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-graphql-api-xray-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-logging
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check

- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-file-system-tagged
- efs-in-backup-plan
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-windows-deployment-type-check
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled

- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- macie-auto-sensitive-data-discovery-check
- mariadb-publish-logs-to-cloudwatch-logs
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check

- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access

- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Mexico (Central) Region

### Mexico (Central)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-redirection-check
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted

- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## Middle East (Bahrain) Region

### Middle East (Bahrain)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged

- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged

- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description

- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check

- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all

- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## Middle East (UAE) Region

### Middle East (UAE)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled

- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled

- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged

- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-enabled

- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

## South America (São Paulo) Region

### South America (São Paulo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-no-environment-variables

- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-enabled
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2-stage-default-route-detailed-metrics-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-rest-api-tagged
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage

- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appflow-flow-trigger-type-check
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-graphql-api-xray-enabled
- appsync-logging-enabled
- aps-rule-groups-namespace-tagged
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged

- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-logins
- cognito-identity-pool-unauth-access-check
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-deletion-protection-enabled
- cognito-user-pool-mfa-enabled
- cognito-user-pool-password-policy-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-location-object-storage-using-https
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check

- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-ml-transform-tagged
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-data-retention
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- kms-key-tagged
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-cluster-tagged
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check

- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check

- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted-in-transit
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check

- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-dlq-check
- sqs-queue-no-public-access
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled
- workspaces-workspace-tagged

## AWS GovCloud (US-East) Region

### AWS GovCloud (US-East)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-redirection-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging
- aurora-resources-protected-by-backup-plan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-environment-privileged-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-report-group-encrypted-at-rest
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami

- ec2-instance-managed-by-ssm
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check

- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-function-public-access-prohibited
- lambda-function-xray-enabled
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access

- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-resources-protected-by-backup-plan
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-enabled
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sqs-queue-dlq-check
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

## AWS GovCloud (US-West) Region

### AWS GovCloud (US-West)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-redirection-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging
- aurora-resources-protected-by-backup-plan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-service-role-check
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- connect-instance-logging-enabled
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-instance-multi-az-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-resources-protected-by-backup-plan

- dynamodb-table-deletion-protection-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-block-public-access
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-last-backup-recovery-point-created
- ec2-launch-templates-ebs-volume-encrypted
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-capacity-provider-termination-check
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-efs-encryption-enabled
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-automatic-backup-check-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-enabled
- elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check

- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-check
- iam-server-certificate-expiration-check
- iam-user-mfa-enabled

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-enabled
- instances-in-vpc
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-function-public-access-prohibited
- lambda-function-xray-enabled
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-log-enabled
- msk-cluster-public-access-disabled
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-resources-protected-by-backup-plan
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sqs-queue-dlq-check
- sqs-queue-policy-full-access-check
- ssm-automation-block-public-sharing

- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

## Creating AWS Config Managed Rules With AWS CloudFormation Templates

> **Important**
>
> You must first create and start the AWS Config configuration recorder in order to create AWS Config managed rules with AWS CloudFormation. For more information, see Managing the Configuration Recorder.

For supported AWS Config managed rules, you can use the CloudFormation templates to create the rule for your account or update an existing CloudFormation stack. A stack is a collection of related resources that you provision and update as a single unit. When you launch a stack with a template, the AWS Config managed rule is created for you. The templates create only the rule, and don't create additional AWS resources.

> **Note**
>
> When AWS Config managed rules are updated, the templates are updated for the latest changes. To save a specific version of a template for a rule, download the template, and upload it to your S3 bucket.

For more information about working with AWS CloudFormation templates, see Getting Started with AWS CloudFormation in the *AWS CloudFormation User Guide*.

**To launch an CloudFormation stack for an AWS Config managed rule**

1. Go to the CloudFormation console and create a new stack.
2. For **Specify template**:
   - If you downloaded the template, choose **Upload a template file**, and then **Choose file** to upload the template.
   - You can also choose **Amazon S3 URL**, and enter the template URL `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/`*`THE_RULE_IDENTIFIER`*`.template`.

   > **Note**
   >
   > The rule identifier should be written in ALL_CAPS_WITH_UNDERSCORES. For example, CLOUDWATCH_LOG_GROUP_ENCRYPTED instead of cloudwatch-log-group-encrypted. For some rules, the rule identifier is different from the rule name. Make sure to use the rule identifier. For example, the rule identifier for restricted-ssh is INCOMING_SSH_DISABLED.

3. Choose **Next**.
4. For **Specify stack details**, type a stack name and enter parameter values for the AWS Config rule. For example, if you are using the `DESIRED_INSTANCE_TYPE` managed rule template, you can specify the instance type such as "m4.large".
5. Choose **Next**.
6. For **Options**, you can create tags or configure other advanced options. These are not required.
7. Choose **Next**.

8. For **Review**, verify that the template, parameters, and other options are correct.
9. Choose **Create**. The stack is created in a few minutes. You can view the created rule in the AWS Config console.

You can use the templates to create a single stack for AWS Config managed rules or update an existing stack in your account. If you delete a stack, the managed rules created from that stack are also deleted. For more information, see Working with Stacks in the *AWS CloudFormation User Guide*.

# AWS Config Custom Rules

AWS Config Custom Rules are rules that you create from scratch. There are two ways to create AWS Config custom rules: with Lambda functions (AWS Lambda Developer Guide) and with Guard (Guard GitHub Repository), a policy-as-code language.

AWS Config custom rules created with Lambda are called *AWS Config Custom Lambda Rules* and AWS Config custom rules created with Guard are called *AWS Config Custom Policy Rules*.

Before using custom rules, see Considerations.

## AWS Config Custom Policy Rules

Rules written using Guard can be created from the AWS Config console or by using the AWS Config rule APIs. AWS Config Custom Policy rules allow you to create AWS Config Custom rules without needing to use Java or Python to develop Lambda functions to manage your custom rules. AWS Config Custom Policy rules are initiated by configuration changes. For more information about Guard, see the Guard GitHub Repository.

## AWS Config Custom Lambda Rules

Custom Lambda rules provide you with the option to use Java or Python to create a Lambda function for a AWS Config Custom rule. A *Lambda function* is custom code that you upload to AWS Lambda, and it is invoked by events that are published to it by an event source. If the Lambda function is associated with an AWS Config rule, AWS Config invokes it when the rule is initiated. The Lambda function then evaluates the configuration information that is sent by AWS Config, and it returns the evaluation results. For more information about Lambda functions, see Function and Event Sources in the *AWS Lambda Developer Guide*.

# Format differences for AWS Config Custom Rules

The following table displays the format differences in the fields for the ConfigurationItem data type and for AWS Config Custom Rules.

| ConfigurationItem | AWS Config Custom Rule |
| --- | --- |
| `version` | `configurationItemVersion` |
| `accountId` | `awsAccountId` |
| `arn` | `ARN` |
| `configurationItemMD5Hash` | `configurationStateMd5Hash` |

**Topics**

- Creating AWS Config Custom Policy Rules
- Creating AWS Config Custom Lambda Rules
- Managing Deleted Resources for AWS Config Custom Lambda Rules

## Creating AWS Config Custom Policy Rules

You can create AWS Config Custom Policy rules from the AWS Management Console, AWS CLI, or AWS Config API.

### Adding AWS Config Custom Policy rules

Using the console

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the Region selector is set to an AWS Region that supports AWS Config rules. For the list of supported Regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. On the **Rules** page, choose **Add rule**.

5. On the **Specify rule type** page, choose **Create custom rule using Guard**.
6. On the **Configure rule** page, create your rule by completing the following steps:
   a. For **Rule name**, type a unique name for the rule.
   b. For **Description**, type a description for the rule.
   c. For **Guard runtime version**, choose the runtime system for your AWS Config Custom Policy rule.
   d. For **Rule Content**, you can populate it with the Guard Custom policy for your rule.
   e. For **Evaluation mode**, choose when in the resource creation and management process you want AWS Config to evaluate your resources. Depending on the rule, AWS Config can evaluate your resource configurations before a resource has been provisioned, after a resource has been provisoned, or both.
      i. Choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.

         After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

         For more information on using this commands, see Evaluating Your Resources with AWS Config Rules. For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.
      ii. Choose **Turn on detective evaluation** to evaluate the configuration settings of your existing resources.

         For detective evaluation, AWS Config Custom Policy rules are initiated by **Configuration changes**. This option will be pre-selected.

         - **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.
         - **Tags** – When a resource with the specified tag is created, changed, or deleted.
         - **All changes** – When a resource recorded by AWS Config is created, changed, or deleted.

AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to constrain which resources initiate evaluations. Otherwise, evaluations are initiated when there is a change to a post-provisioned resource.

f. For **Parameters**, you can customize the values for the provided keys if your rule includes parameters. A parameter is an attribute that your resources must adhere to before they are considered compliant with the rule.

7. On the **Review and create** page, review all your selections before adding the rule to your AWS account.
8. When you finish reviewing your rules, choose **Add rule**.

Using the AWS CLI

Use the `put-config-rule` command.

The `Owner` field should be `CUSTOM_POLICY`. The following additional fields are required for AWS Config Custom Policy rules:

- `Runtime`: The runtime system for your AWS Config Custom Policy rules.
- `PolicyText`: The policy definition containing the logic for your AWS Config Custom Policy rules.
- `EnableDebugLogDelivery`: The Boolean expression for enabling debug logging for your AWS Config Custom Policy rule. The default value is `false`.

Using the API Reference

Use the PutConfigRule action.

The `Owner` field should be `CUSTOM_POLICY`. The following additional fields are required for AWS Config Custom Policy rules:

- `Runtime`: The runtime system for your AWS Config Custom Policy rules.
- `PolicyText`: The policy definition containing the logic for your AWS Config Custom Policy rules.

- `EnableDebugLogDelivery`: The Boolean expression for enabling debug logging for your AWS Config Custom Policy rule. The default value is `false`.

## Writing rule content for AWS Config Custom Policy rules

With AWS Config Custom Policy rules, you can use AWS CloudFormation Guard's domain-specific language (DSL) to evaluate resource configurations. This topic provides patterns and best practices for writing custom policy rules.

For more information on how to write rules with Guard, see Writing Guard rules in the AWS CloudFormation Guard User Guide and AWS CloudFormation Guard 2.0's Modes of Operation in the Guard GitHub Repository.

### Basic rule structure

Use the following basic format to create rules:

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
    %resources_of_type.configuration.property == expected_value
}
```

### Key components

configuration

Contains the contents for the resource configuration.

supplementaryConfiguration

Contains additional contents for the resource configuration. AWS Config returns this field for certain resource types to supplement the information returned for the configuration field.

resourceType

AWS resource type being evaluated.

resourceId

The ID of the resource (for example, `sg-xxxxxx`).

accountId

The 12-digit AWS account ID associated with the resource.

### Common patterns

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
    property1 exists
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
```

```
}
```

### Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

## Advanced features

### Range checks

```
rule check_numeric_limits {
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

### Combining conditions

```
# AND conditions (implicit through new lines)
condition_1
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

### Chaining rules

```
rule check_prerequisites {
```

```
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

### Best practices

- Use variables with `let` statements for improved readability.
- Group related checks using named rule blocks.
- Include descriptive comments.
- Use appropriate operators (`exists`, `is_string`, `is_list`).
- Use regex patterns with case-insensitive matching.

### Example: dynamodb-pitr-enabled

The following example shows the policy definition for an AWS Config Custom Policy rule version of the AWS Config Managed rule dynamodb-pitr-enabled. This rule checks if DynamoDB tables have Point-in-Time Recovery enabled.

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

# Creating AWS Config Custom Lambda Rules

You can develop custom rules and add them to AWS Config with AWS Lambda functions.

You associate each custom rule with an Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule. You associate this function with your rule, and the rule invokes the function either in response to configuration changes or periodically. The function then evaluates whether your resources comply with your rule, and sends its evaluation results to AWS Config.

**AWS Rule Development Kit (RDK)**

The AWS Rule Development Kit (RDK) is designed to support a "Compliance-as-Code" workflow that is intuitive and productive. It abstracts away much of the undifferentiated heavy lifting associated with deploying AWS Config rules backed by custom Lambda functions, and provides a streamlined develop-deploy-monitor iterative process.

For step-by-step instruction, see the AWS Rule Development Kit (RDK) Documentation.

**Example AWS Lambda Functions for AWS Config Rules (Node.js)**

AWS Lambda executes functions in response to events that are published by AWS services. The function for an AWS Config Custom Lambda rule receives an event that is published by AWS Config, and the function then uses data that it receives from the event and that it retrieves from the AWS Config API to evaluate the compliance of the rule. The operations in a function for a Config rule differ depending on whether it performs an evaluation that is triggered by configuration changes or triggered periodically.

For information about common patterns within AWS Lambda functions, see Programming Model in the *AWS Lambda Developer Guide*.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config will invoke a function like the following example when it detects a configuration change for a resource that is within a custom rule's scope.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Configuration changes** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ConfigurationItemChangeNotification` and

`OversizedConfigurationItemChangeNotification`. These settings enable your rule to be triggered whenever AWS Config generates a configuration item or an oversized configuration item as a result of a resource change.

This example evaluates your resources and checks whether the instances match the resource type, `AWS::EC2::Instance`. The rule is triggered when AWS Config generates a configuration item or an oversized configuration item notification.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory
 API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
```

```
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem)
 => {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
```

```
}

// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}

// In this example, the resource is compliant if it is an instance and its type
 matches the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration,
 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
```

```
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
 not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

### Function Operations

The function performs the following operations at runtime:

1. The function runs when AWS Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to

return information to the caller. AWS Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.

2. The function checks whether the `messageType` for the event is a configuration item or an oversized configuration item, and then returns the configuration item.
3. The handler calls the `isApplicable` function to determine whether the resource was deleted.

> **Note**
>
> Rules reporting on deleted resources should return the evaluation result of `NOT_APPLICABLE` in order to avoid unnecessary rule evaluations.

4. The handler calls the `evaluateChangeNotificationCompliance` function and passes the `configurationItem` and `ruleParameters` objects that AWS Config published in the event.

   The function first evaluates whether the resource is an EC2 instance. If the resource is not an EC2 instance, the function returns a compliance value of `NOT_APPLICABLE`.

   The function then evaluates whether the `instanceType` attribute in the configuration item is equal to the `desiredInstanceType` parameter value. If the values are equal, the function returns `COMPLIANT`. If the values are not equal, the function returns `NON_COMPLIANT`.
5. The handler prepares to send the evaluation results to AWS Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result, the resource type, and the ID of the resource that was evaluated. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for AWS Config.
6. The handler sends the evaluation results to AWS Config by passing the object to the `putEvaluations` method of the `config` client.

### Example Function for Periodic Evaluations

AWS Config will invoke a function like the following example for periodic evaluations. Periodic evaluations occur at the frequency that you specify when you define the rule in AWS Config.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Periodic** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ScheduledNotification`.

This example checks whether the total number of a specified resource exceeds a specified maximum.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON
 objects passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount,
 count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not
 compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
```

```
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
```

```
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
```

```
}
```

### Function Operations

The function performs the following operations at runtime:

1. The function runs when AWS Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller. AWS Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.
2. To count the resources of the specified type, the handler calls the `countResourceTypes` function, and it passes the `applicableResourceType` parameter that it received from the event. The `countResourceTypes` function calls the `listDiscoveredResources` method of the `config` client, which returns a list of identifiers for the applicable resources. The function uses the length of this list to determine the number of applicable resources, and it returns this count to the handler.
3. The handler prepares to send the evaluation results to AWS Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result and the AWS account that was published in the event. You can use the `Evaluations` parameter to apply the result to any resource type that is supported by AWS Config. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for AWS Config.
4. Within the `putEvaluationsRequest` object, the handler calls the `evaluateCompliance` function. This function tests whether the number of applicable resources exceeds the maximum assigned to the `maxCount` parameter, which was provided by the event. If the number of resources exceeds the maximum, the function returns `NON_COMPLIANT`. If the number of resources does not exceed the maximum, the function returns `COMPLIANT`.
5. The handler sends the evaluation results to AWS Config by passing the object to the `putEvaluations` method of the `config` client.

## Example AWS Lambda Functions for AWS Config Rules (Python)

AWS Lambda executes functions in response to events that are published by AWS services. The function for an AWS Config Custom Lambda rule receives an event that is published by AWS Config, and the function then uses data that it receives from the event and that it retrieves from the AWS Config API to evaluate the compliance of the rule. The operations in a function

for a Config rule differ depending on whether it performs an evaluation that is triggered by configuration changes or triggered periodically.

For information about common patterns within AWS Lambda functions, see Programming Model in the *AWS Lambda Developer Guide*.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config will invoke a function like the following example when it detects a configuration change for a resource that is within a custom rule's scope.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Configuration changes** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ConfigurationItemChangeNotification` and `OversizedConfigurationItemChangeNotification`. These settings enable your rule to be triggered whenever AWS Config generates a configuration item or an oversized configuration item as a result of a resource change.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
```

```
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
```

```
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
```

```
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
```

```
        ],
        ResultToken=event['resultToken'])
```

### Function Operations

The function performs the following operations at runtime:

1. The function runs when AWS Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller. AWS Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.
2. The function checks whether the `messageType` for the event is a configuration item or an oversized configuration item, and then returns the configuration item.
3. The handler calls the `isApplicable` function to determine whether the resource was deleted.

   > **Note**
   >
   > Rules reporting on deleted resources should return the evaluation result of `NOT_APPLICABLE` in order to avoid unnecessary rule evaluations.

4. The handler calls the `evaluateChangeNotificationCompliance` function and passes the `configurationItem` and `ruleParameters` objects that AWS Config published in the event.

   The function first evaluates whether the resource is an EC2 instance. If the resource is not an EC2 instance, the function returns a compliance value of `NOT_APPLICABLE`.

   The function then evaluates whether the `instanceType` attribute in the configuration item is equal to the `desiredInstanceType` parameter value. If the values are equal, the function returns `COMPLIANT`. If the values are not equal, the function returns `NON_COMPLIANT`.
5. The handler prepares to send the evaluation results to AWS Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result, the resource type, and the ID of the resource that was evaluated. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for AWS Config.

6. The handler sends the evaluation results to AWS Config by passing the object to the `putEvaluations` method of the `config` client.

## Example Function for Periodic Evaluations

AWS Config will invoke a function like the following example for periodic evaluations. Periodic evaluations occur at the frequency that you specify when you define the rule in AWS Config.

If you use the AWS Config console to create a rule that is associated with a function like this example, choose **Periodic** as the trigger type. If you use the AWS Config API or AWS CLI to create the rule, set the `MessageType` attribute to `ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
```

```
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
    Keyword arguments:
```

```
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
```

```
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

### Function Operations

The function performs the following operations at runtime:

1. The function runs when AWS Lambda passes the `event` object to the `handler` function. In this example, the function accepts the optional `callback` parameter, which it uses to return information to the caller. AWS Lambda also passes a `context` object, which contains information and methods that the function can use while it runs. Note that in newer versions of Lambda, context is no longer used.
2. To count the resources of the specified type, the handler calls the `countResourceTypes` function, and it passes the `applicableResourceType` parameter that it received from the event. The `countResourceTypes` function calls the `listDiscoveredResources` method of the `config` client, which returns a list of identifiers for the applicable resources. The function uses the length of this list to determine the number of applicable resources, and it returns this count to the handler.
3. The handler prepares to send the evaluation results to AWS Config by initializing the `putEvaluationsRequest` object. This object includes the `Evaluations` parameter, which identifies the compliance result and the AWS account that was published in the event. You can use the `Evaluations` parameter to apply the result to any resource type that is supported by AWS Config. The `putEvaluationsRequest` object also includes the result token from the event, which identifies the rule and the event for AWS Config.
4. Within the `putEvaluationsRequest` object, the handler calls the `evaluateCompliance` function. This function tests whether the number of applicable resources exceeds the maximum assigned to the `maxCount` parameter, which was provided by the event. If the number of resources exceeds the maximum, the function returns `NON_COMPLIANT`. If the number of resources does not exceed the maximum, the function returns `COMPLIANT`.
5. The handler sends the evaluation results to AWS Config by passing the object to the `putEvaluations` method of the `config` client.

### Example Events for AWS Config Rules

When the trigger for a rule occurs, AWS Config invokes the rule's AWS Lambda function by publishing an event. Then AWS Lambda executes the function by passing the event to the function's handler.

Example Event for Evaluations Triggered by Configuration Changes

AWS Config publishes an event when it detects a configuration change for a resource that is within a rule's scope. The following example event shows that the rule was triggered by a configuration change for an EC2 instance.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

Some resource changes generate oversized configuration items. The following example event shows that the rule was triggered by an oversized configuration change for an EC2 instance.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
```

```
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

AWS Config publishes an event when it evaluates your resources at a frequency that you specify (such as every 24 hours). The following example event shows that the rule was triggered by a periodic frequency.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

### Event Attributes

The JSON object for an AWS Config event contains the following attributes:

`invokingEvent`

The event that triggers the evaluation for a rule. If the event is published in response to a resource configuration change, the value for this attribute is a string that contains a JSON `configurationItem` or a `configurationItemSummary` (for oversized configuration items). The configuration item represents the state of the resource at the moment that AWS Config detected the change. For an example of a configuration item, see the output produced by the `get-resource-config-history` AWS CLI command in Viewing Configuration History.

If the event is published for a periodic evaluation, the value is a string that contains a JSON object. The object includes information about the evaluation that was triggered.

For each type of event, a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Key/value pairs that the function processes as part of its evaluation logic. You define parameters when you use the AWS Config console to create a Custom Lambda rule. You can also define parameters with the `InputParameters` attribute in the `PutConfigRule` AWS Config API request or the `put-config-rule` AWS CLI command.

The JSON code for the parameters is contained within a string, so a function must parse the string with a JSON parser to be able to evaluate its contents, as shown in the following Node.js example:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

A token that the function must pass to AWS Config with the `PutEvaluations` call.

`eventLeftScope`

A Boolean value that indicates whether the AWS resource to be evaluated has been removed from the rule's scope. If the value is `true`, the function indicates that the evaluation can be

ignored by passing `NOT_APPLICABLE` as the value for the `ComplianceType` attribute in the `PutEvaluations` call.

`executionRoleArn`

The ARN of the IAM role that is assigned to AWS Config.

`configRuleArn`

The ARN that AWS Config assigned to the rule.

`configRuleName`

The name that you assigned to the rule that caused AWS Config to publish the event and invoke the function.

`configRuleId`

The ID that AWS Config assigned to the rule.

`accountId`

The ID of the AWS account that owns the rule.

`version`

A version number assigned by AWS. The version will increment if AWS adds attributes to AWS Config events. If a function requires an attribute that is only in events that match or exceed a specific version, then that function can check the value of this attribute.

The current version for AWS Config events is 1.0.

## Managing Deleted Resources for AWS Config Custom Lambda Rules

Rules reporting on deleted resources should return the evaluation result of `NOT_APPLICABLE` in order to avoid unnecessary rule evaluations.

When you delete a resource, AWS Config creates a `configurationItem` with `ResourceDeleted` for the `configurationItemStatus`. You can use this metadata to check if a rule reports on a deleted resource. For more information on configuration items, see Concepts | Configuration Items.

Include the following code snippets to check for deleted resources and set the evaluation result of an AWS Config custom lambda rule to `NOT_APPLICABLE` if it reports on a deleted resource:

### Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

### Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

**Note**

AWS Config managed rules and AWS Config custom policy rules handle this behavior by default.

If you create an AWS Config custom lambd rule with Python using the AWS Config Development Kit (RDK) and AWS Config Development Kit Library (RDKlib), the imported Evaluator class will check this behavior. For information on how to write rules with the RDK and RDKlib, see Writing rules with the RDK and RDKlib.

# Service-Linked AWS Config Rules

A service-linked AWS Config rule is a unique type of AWS Config managed rules that supports other AWS services to create AWS Config rules in your account. Service-linked rules are predefined to include all the permissions required to call other AWS services on your behalf. These rules are similar to standards that an AWS service recommends in your AWS account for compliance verification.

These service-linked AWS Config rules are owned by AWS service teams. The AWS service team creates these rules in your AWS account. You have read-only access to these rules. You cannot edit or delete these rules if you are subscribed to AWS service that these rules are linked to.

**Service-linked rules and the AWS Command Line Interface**

With the AWS CLI, the PutConfigRule, DeleteConfigRule, and DeleteEvaluationResults APIs return access denied with the following error message:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

**Service-linked rules and the AWS Config console**

In the AWS Config console, the service-linked AWS Config rules are visible in the **Rules** page. The **Edit** and **Delete results** buttons are greyed in the console to restrict you from editing the rule. You can view details of the rule by choosing the rule.

**Service-linked rules, remediation actions, and conformance packs**

To add remediation actions to a service-linked rules in a conformance pack, you need to add the remediation action to the conformance pack template itself, and then update the conformance pack with your updated template. For information on updating conformance packs, see Deploying a Conformance Pack (Console), Deploying a Conformance Pack (AWS CLI) and Managing Organizational Conformance Packs.

**Editing and deleting service-linked rules**

To edit or delete a service-linked rule, contact the AWS service that created the rule. For example, for service-linked rules created by AWS Security Hub CSPM, you can remove a service-linked rule by following these steps in the *AWS Security Hub CSPM User Guide*: Disabling a security standard.

# Managing AWS Config Rules Across All Accounts in Your Organization

> **Important**
>
> Organizational rules can only be created using the API or CLI. This operation is not supported in the AWS Config console.

AWS Config allows you to manage AWS Config rules across all AWS accounts within an organization. You can:

- Centrally create, update, and delete AWS Config rules across all accounts in your organization.
- Deploy a common set of AWS Config rules across all accounts and specify accounts where AWS Config rules should not be created.
- Use the APIs from the management account in AWS Organizations to enforce governance by ensuring that the underlying AWS Config rules are not modifiable by your organization's member accounts.

## Considerations

### For deployments across different regions

The API call to deploy rules and conformance packs across accounts is AWS Region specific. At the organization level, you need to change the context of your API call to a different region if you want to deploy rules in other regions. For example, to deploy a rule in US East (N. Virginia), change the region to US East (N. Virginia) and then call `PutOrganizationConfigRule`.

### For accounts within an organization

If a new account joins an organization, the rule or conformance pack is deployed to that account. When an account leaves an organization, the rule or conformance pack is removed.

If you deploy an organizational rule or conformance pack in an organization administrator account, and then establish a delegated administrator and deploy an organizational rule or conformance pack in the delegated administrator account, you won't be able to see the organizational rule or conformance pack in the organization administrator account from the delegated administrator

account or see the organizational rule or conformance pack in the delegated administrator account from organization administrator account. The DescribeOrganizationConfigRules and DescribeOrganizationConformancePacks APIs can only see and interact with the organization-related resource that were deployed from within the account calling those APIs.

**Retry mechanism for new accounts added to an organization**

Deployment of existing organizational rules and conformance packs will only be retried for 7 hours after an account is added to your organization if a recorder is not available. You are expected to create a recorder if one doesn't exist within 7 hours of adding an account to your organization.

**Organization management accounts, delegated administrators, and service-linked roles**

If you are using an organization management account and intend to use a delegated administrator for organizational deployment, be aware that AWS Config won't automatically create the service-linked role (SLR). You must manually create the service-linked role (SLR) separately using IAM.

If you do not have an SLR for your management account, you will not be able to deploy resources to that account from a delegated administrator account. You will still be able to deploy AWS Config rules to member accounts from management and delegated administrator accounts. For more information, see Using service-linked roles in the *AWS Identity and Access Management (IAM) User Guide*.

## Deployment

For information on how to integrate AWS Config with AWS Organizations, see AWS Config and AWS Organizations in the *AWS Organizations User Guide*. Ensure AWS Config recording is on before you use the following APIs to manage AWS Config rules across all AWS accounts within an organization:

- PutOrganizationConfigRule, adds or updates organization config rule for your entire organization evaluating whether your AWS resources comply with your desired configurations.
- DescribeOrganizationConfigRules, returns a list of organization config rules.
- GetOrganizationConfigRuleDetailedStatus, returns detailed status for each member account within an organization for a given organization config rule.
- GetOrganizationCustomRulePolicy, returns the policy definition containing the logic for your organization config custom policy rule.
- DescribeOrganizationConfigRuleStatuses, provides organization config rule deployment status for an organization.

- DeleteOrganizationConfigRule, deletes the specified organization config rule and all of its evaluation results from all member accounts in that organization.

## Region Support

Deploying AWS Config Rules across member accounts in an AWS Organization is supported in the following Regions.

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| (Hyderabad) | | | |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS | |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS | |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS | |
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS | |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS | |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS | |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS | |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS | |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS | |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# Adding AWS Config Rules

You can use the AWS Config console or the AWS SDKs to add rules.

**Topics**

- Adding Rules (Console)
- Adding Rules (AWS SDKs)

## Adding Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until AWS Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When AWS Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your AWS Resources with AWS Config.

> **Note**
>
> When you add a new rule, AWS Config evaluates the applicable resources in your resource inventory, including previously recorded resources. For example, if you recorded

`AWS::IoT::Policy` resources but later excluded them from recording, AWS Config retains the initial configuration items (CIs) in your inventory. Although AWS Config no longer updates these CIs when their associated resource types are excluded from recording, it retains their last recorded state and evaluates them when you add applicable rules.
AWS Config does not evaluate resources that are not in the resource inventory. For example, if you add the amplify-branch-tagged rule but don't record and have never recorded `AWS::Amplify::Branch` resources, AWS Config can't evaluate whether the AWS Amplify branches in your account are compliant or noncompliant.
For more information, see Recording AWS Resources with AWS Config.

### Adding rules

#### To add a rule

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. On the **Rules** page, choose **Add rule**.
5. On the **Specify rule type** page, specify the rule type by completing the following steps:
   a. Type in the search field to filter the list of managed rules by rule name, description, and label. For example, type **EC2** to return rules that evaluate EC2 resource types or type **periodic** to return rules that are triggered periodically.
   b. You can also create your own custom rule. Choose **Create custom rule using Lambda** or **Create custom rule using Guard**, and follow the procedure in Creating AWS Config Custom Lambda Rules or Creating AWS Config Custom Policy Rules.
6. On the **Configure rule** page, configure your rule by completing the following steps:
   a. For **Name**, type a unique name for the rule.
   b. For **Description**, type a description for the rule.
   c. For **Evaluation mode**, choose when in the resource creation and management process you want AWS Config to evaluate your resources. Depending on the rule, AWS Config

can evaluate your resource configurations before a resource has been deployed, after a resource has been deployed, or both.

i. Choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.

   After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

   For more information on using this commands, see Evaluating Your Resources with AWS Config Rules. For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.

ii. Choose **Turn on detective evaluation** to evaluate the configuration settings of your existing resources.

   For detective evaluation, there are two types of triggers: **When configuration changes** and **Periodic**.

   A. If the trigger types for your rule include **Configuration changes**, specify one of the following options for **Scope of changes** with which AWS Config invokes your Lambda function:

      - **Resources** – When a resource that matches the specified resource type, or the type plus identifier, is created, changed, or deleted.
      - **Tags** – When a resource with the specified tag is created, changed, or deleted.
      - **All changes** – When a resource recorded by AWS Config is created, changed, or deleted.

      AWS Config runs the evaluation when it detects a change to a resource that matches the rule's scope. You can use the scope to define which resources initiate evaluations.

   B. If the trigger types for your rule include **Periodic**, specify the **Frequency** with which AWS Config invokes your Lambda function.

d. For **Parameters**, you can customize the values for the provided keys if your rule includes parameters. A parameter is an attribute that your resources must adhere to before they are considered compliant with the rule.

7. On the **Review and create** page, review all your selections before adding the rule to your AWS account. If your rule is not working as expected, you might see one of the following for **Compliance**:

   - **No results reported** - AWS Config evaluated your resources against the rule. The rule did not apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation results were deleted. To get evaluation results, update the rule, change its scope, or choose **Re-evaluate**.

     This message may also appear if the rule didn't report evaluation results.
   - **No resources in scope** - AWS Config cannot evaluate your recorded AWS resources against this rule because none of your resources are within the rule's scope. To get evaluation results, edit the rule and change its scope, or add resources for AWS Config to record by using the **Settings** page.
   - **Evaluations failed** - For information that can help you determine the problem, choose the rule name to open its details page and see the error message.

## Adding Rules (AWS SDKs)

### Adding rules

The following code examples show how to use `PutConfigRule`.

CLI

**AWS CLI**

**To add an AWS managed Config rule**

The following command provides JSON code to add an AWS managed Config rule:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so AWS Config will evaluate only EC2 instances against the rule. Because the rule is a managed rule, the `Owner` attribute is set to `AWS`, and the `SourceIdentifier` attribute is set to the rule identifier, `REQUIRED_TAGS`. For the `InputParameters` attribute, the tag keys that the rule requires, `CostCenter` and `Owner`, are specified.

If the command succeeds, AWS Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

**To add a customer managed Config rule**

The following command provides JSON code to add a customer managed Config rule:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
```

```
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so AWS Config will evaluate only EC2 instances against the rule. Because this rule is a customer managed rule, the `Owner` attribute is set to `CUSTOM_LAMBDA`, and the `SourceIdentifier` attribute is set to the ARN of the AWS Lambda function. The `SourceDetails` object is required. The parameters that are specified for the `InputParameters` attribute are passed to the AWS Lambda function when AWS Config invokes it to evaluate resources against the rule.

If the command succeeds, AWS Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

- For API details, see PutConfigRule in *AWS CLI Command Reference*.

Python

**SDK for Python (Boto3)**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class ConfigWrapper:
    """
```

```
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- For API details, see PutConfigRule in *AWS SDK for Python (Boto3) API Reference*.

# Updating AWS Config Rules

You can use the AWS Config console or the AWS SDKs to update your rules.

**Topics**


- Updating Rules (Console)
- Updating Rules (AWS SDKs)


## Updating Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until AWS Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When AWS Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your AWS Resources with AWS Config.

### Updating rules

**To update a rule**

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. Choose a rule and **Edit rule** for the rule that you want to update.
5. Modify the settings on the **Edit rule** page to change your rule as needed.
6. Choose **Save**.

## Updating Rules (AWS SDKs)

### Updating rules

If you are updating a rule that you added previously, you can specify the rule by `ConfigRuleName`, `ConfigRuleId`, or `ConfigRuleArn` in the `ConfigRule` data type that you use in this request. You use the same `PutConfigRule` command that you use when adding a rule.

The following code examples show how to use `PutConfigRule`.

CLI

### AWS CLI

#### To add an AWS managed Config rule

The following command provides JSON code to add an AWS managed Config rule:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so AWS Config will evaluate only EC2 instances against the rule. Because the rule is a managed rule, the `Owner` attribute is set to `AWS`, and the `SourceIdentifier` attribute is set to the rule identifier, `REQUIRED_TAGS`. For the `InputParameters` attribute, the tag keys that the rule requires, `CostCenter` and `Owner`, are specified.

If the command succeeds, AWS Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

#### To add a customer managed Config rule

The following command provides JSON code to add a customer managed Config rule:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so AWS Config will evaluate only EC2 instances against the rule. Because this rule is a customer managed rule, the `Owner` attribute is set to `CUSTOM_LAMBDA`, and the `SourceIdentifier` attribute is set to the ARN of the AWS Lambda function. The `SourceDetails` object is required. The parameters that are specified for the `InputParameters` attribute are passed to the AWS Lambda function when AWS Config invokes it to evaluate resources against the rule.

If the command succeeds, AWS Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

- For API details, see PutConfigRule in *AWS CLI Command Reference*.

Python

### SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
```

```
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- For API details, see PutConfigRule in *AWS SDK for Python (Boto3) API Reference*.

# Deleting AWS Config Rules

You can use the AWS Config console or the AWS SDKs to delete your rules.

**Topics**


- Considerations
- Deleting Rules (Console)
- Deleting Rules (AWS SDKs)


## Considerations

**Recommendation: Consider excluding the `AWS::Config::ResourceCompliance` resource type from recording before deleting rules**

Deleting rules creates configuration items (CIs) for `AWS::Config::ResourceCompliance` that can affect your costs for the configuration recorder. If you are deleting rules which evaluate a large number of resource types, this can lead to a spike in the number of CIs recorded.

To avoid the associated costs, you can opt to disable recording for the `AWS::Config::ResourceCompliance` resource type before deleting rules, and re-enable recording after the rules have been deleted.

However, since deleting rules is an asynchronous process, it might take an hour or more to complete. During the time when recording is disabled for `AWS::Config::ResourceCompliance`, rule evaluations will not be recorded in the associated resource's history.

## Deleting Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until AWS Config finishes evaluating your resources against the rule. You can update the results with the refresh button. When AWS Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your AWS Resources with AWS Config.

> **Note**
>
> AWS Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, AWS Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see Recording AWS Resources with AWS Config.

#### Deleting rules

#### To delete a rule

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. Choose a rule from the table that you want to delete.
5. From the **Actions** dropdown list, choose **Delete rule**.
6. When prompted, type "Delete" (case-sensitive) and then choose **Delete**.

# Deleting Rules (AWS SDKs)

## Deleting rules

The following code examples show how to use `DeleteConfigRule`.

CLI

### AWS CLI

#### To delete an AWS Config rule

The following command deletes an AWS Config rule named `MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- For API details, see DeleteConfigRule in *AWS CLI Command Reference*.

Python

### SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- For API details, see DeleteConfigRule in *AWS SDK for Python (Boto3) API Reference*.

# Viewing Details and Compliance Information for your AWS Config Rules

> **Important**
>
> For accurate reporting on the compliance status, you must record the `AWS::Config::ResourceCompliance` resource type. For more information, see Recording AWS Resources.

You can use the AWS Config console or the AWS SDKs to view your rules.

**Topics**

- Viewing Rules (Console)
- Viewing Rules (AWS SDKs)

## Viewing Rules (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until AWS Config finishes evaluating your resources against the rule. You can

update the results with the refresh button. When AWS Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your AWS Resources with AWS Config.

> **Note**
>
> AWS Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, AWS Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see Recording AWS Resources with AWS Config.

### Viewing rules

#### To view your rules

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the region selector is set to a region that supports AWS Config rules. For the list of supported regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**.
4. The **Rules** page shows all the rule that are currently in your AWS account. It lists the name, associated remediation action, and compliance status of each rule.
   - Choose **Add rule** to get started with creating a rule.
   - Choose a rule to see its settings, or choose a rule and **View details**.
   - See the compliance status of the rule when it evaluates your resources.
   - Choose a rule and **Edit rule** to change the configuration settings of the rule and set a remediation action for a noncompliant rule.

## Viewing Rules (AWS SDKs)

### Viewing details for your rules

The following code examples show how to use `DescribeConfigRules`.

CLI

## AWS CLI

### To get details for an AWS Config rule

The following command returns details for an AWS Config rule named `InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
```

```
}
```

- For API details, see DescribeConfigRules in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This sample lists config rules for the account, with selected properties.**

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

**Output:**

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This sample lists config rules for the account, with selected properties.**

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

**Output:**

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                      ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                               config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                 config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required          config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

## Python

### SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- For API details, see DescribeConfigRules in *AWS SDK for Python (Boto3) API Reference*.

### Viewing compliance information for your rules

The following code examples show how to use `DescribeComplianceByConfigRule`.

CLI

#### AWS CLI

**To get compliance information for your AWS Config rules**

The following command returns compliance information for each AWS Config rule that is violated by one or more AWS resources:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many resources do not comply with the related rule. For example, the following output indicates that 3 resources do not comply with the rule named `InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- For API details, see DescribeComplianceByConfigRule in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA**

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

**Output:**

```
ComplianceContributorCount ComplianceType
```

```
-------------------------- --------------
                           INSUFFICIENT_DATA
```

**Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.**

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA**

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

**Output:**

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

**Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.**

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

### Viewing the compliance summary for your rules

The following code examples show how to use `GetComplianceSummaryByConfigRule`.

CLI

#### AWS CLI

**To get the compliance summary for your AWS Config rules**

The following command returns the number of rules that are compliant and the number that are noncompliant:

```
aws configservice get-compliance-summary-by-config-rule
```

In the output, the value for each `CappedCount` attribute indicates how many rules are compliant or noncompliant.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
```

```
}
```

- For API details, see GetComplianceSummaryByConfigRule in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This sample returns the number of Config rules that are non-compliant.**

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This sample returns the number of Config rules that are non-compliant.**

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

### Viewing the evaluation results for your rules

The following code examples show how to use `GetComplianceDetailsByConfigRule`.

CLI

## AWS CLI

### To get the evaluation results for an AWS Config rule

The following command returns the evaluation results for all of the resources that don't comply with an AWS Config rule named `InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- For API details, see GetComplianceDetailsByConfigRule in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

**Output:**

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

**Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

**Output:**

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

**Output:**

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

**Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

**Output:**

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

# Turning on Proactive Evaluation for AWS Config Rules

You can use the AWS Config console or the AWS SDKs to turn on proactive evaluation rules. For a list of resource types and managed rules that support proactive evaluation, see Components of a Rule | Evaluation Modes.

**Topics**


- Turning on Proactive Evaluation (Console)
- Turning on Proactive Evaluation (AWS SDKs)


## Turning on Proactive Evaluation (Console)

The **Rules** page shows your rules and their current compliance results in a table. The result for each rule is **Evaluating...** until AWS Config finishes evaluating your resources against the rule. You can update the results with the refresh button.

When AWS Config finishes evaluations, you can see the rules and resource types that are compliant or noncompliant. For more information, see Viewing Compliance Information and Evaluation Results for your AWS Resources with AWS Config.

> **Note**
>
> AWS Config evaluates only the resource types that it is recording. For example, if you add the **cloudtrail-enabled** rule but don't record the CloudTrail trail resource type, AWS Config can't evaluate whether the trails in your account are compliant or noncompliant. For more information, see Recording AWS Resources with AWS Config.

### Turning on proactive evaluation

You can use *proactive evaluation* to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*AWS public extensions*" within the AWS CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the CloudFormation registry and AWS resource and property types reference in the AWS CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

#### To turn on proactive evalution

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the Region selector is set to a Region that supports AWS Config rules. For the list of supported AWS Regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**. For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.
4. Choose a rule, and then choose **Edit rule** for the rule that you want to update.
5. For **Evaluation mode**, choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.
6. Choose **Save**.

After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

For example, start with the StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the GetResourceEvaluationSummary API to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
```

```
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the GetComplianceDetailsByResource API.

## Turning on Proactive Evaluation (AWS SDKs)

### Turning on proactive evaluation (AWS CLI)

You can use *proactive evaluation* to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*AWS public extensions*" within the AWS CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the CloudFormation registry and AWS resource and property types reference in the AWS CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

#### To turn on proactive evaluation

Use the `put-config-rule` command and enable `PROACTIVE` for `EvaluationModes`.

After you have turned on proactive evaluation, you can use the start-resource-evaluation CLI command and get-resource-evaluation-summary CLI command to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

For example, start with the **start-resource-evaluation** command:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the **get-resource-evaluation-summary** to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the get-compliance-details-by-resource CLI command.

> **Note**
>
> For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.

### Turning on proactive evaluation (API)

You can use *proactive evaluation* to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*AWS public extensions*" within the AWS CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the CloudFormation registry and AWS resource and property types reference in the AWS CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

### To turn on proactive evaluation for a rule

Use the PutConfigRule action and enable `PROACTIVE` for `EvaluationModes`.

After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region. For example, start with the StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the GetResourceEvaluationSummary API to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the GetComplianceDetailsByResource API.

> **Note**
>
> For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.

# Sending Rule Evaluations to Security Hub CSPM

After adding an AWS Config rule, you can also send rule evaluations to AWS Security Hub CSPM. The integration between AWS Config and Security Hub CSPM allows you to triage and remediate rule evaluations alongside other misconfigurations and security issues.

## Send Rule Evaluations to Security Hub CSPM

To send rule evaluations to Security Hub CSPM, you must first set up AWS Security Hub CSPM and AWS Config, and then add at least one AWS Config managed or custom rule. After this, AWS Config immediately starts sending rule evaluations to Security Hub CSPM. Security Hub CSPM enriches the rule evaluations and transforms them into Security Hub CSPM findings.

For more information about this integration, see Available AWS Service Integrations in the AWS Security Hub CSPM User Guide.

# Evaluating Your Resources with AWS Config Rules

When you create custom rules or use managed rules, AWS Config evaluates your resources against those rules. You can run on-demand evaluations for resources against your rules. For example, this is helpful when you create a custom rule and want to check that AWS Config is correctly evaluating your resources or to identify if there is an issue with the evaluation logic of your AWS Lambda function.

**Example**

1. You create a custom rule that evaluates whether your IAM users have active access keys.
2. AWS Config evaluates your resources against your custom rule.
3. An IAM user who doesn't have an active access key exists in your account. Your rule doesn't correctly flag this resource as NON_COMPLIANT.
4. You fix the rule and start the evaluation again.

5. Because you fixed your rule, the rule correctly evaluates your resources, and flags the IAM user resource as NON_COMPLIANT.

When you add a rule to your account, you can specify when in the resource creation and management process that you want AWS Config to evaluate your resources. The resource creation and management process is known as resource provisioning. You choose the *evaluation mode* to specify when in this process you want AWS Config to evaluate your resources.

Depending on the rule, AWS Config can evaluate your resource configurations before a resource has been deployed, after a resource has been deployed, or both. Evaluating a resource before it has been deployed is **proactive evaluation**. Evaluating a resource after it has been deployed is **detective evaluation**.

## Proactive mode

Use proactive evaluation to evaluate resources before they have been deployed. This allows you to evaluate whether a set of resource properties, if used to define an AWS resource, would be COMPLIANT or NON_COMPLIANT given the set of proactive rules that you have in your account in your Region.

The Resource type schema states the properties of a resource. You can find the resource type schema in "*AWS public extensions*" within the AWS CloudFormation registry or with the following CLI commmand:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

For more information, see Managing extensions through the CloudFormation registry and AWS resource and property types reference in the AWS CloudFormation User Guide.

> **Note**
>
> Proactive rules do not remediate resources that are flagged as NON_COMPLIANT or prevent them from being deployed.

### Evaluating your Resources

#### To turn on proactive evalution

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the Region selector is set to a Region that supports AWS Config rules. For the list of supported AWS Regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the left navigation, choose **Rules**. For a list of managed rules that support proactive evaluation, see List of AWS Config Managed Rules by Evaluation Mode.
4. Choose a rule, and then choose **Edit rule** for the rule that you want to update.
5. For **Evaluation mode**, choose **Turn on proactive evaluation** to allow you to run evaluations on the configuration settings of your resources before they are deployed.
6. Choose **Save**.

> **Note**
>
> You can also turn on proactive evaluation using the `put-config-rule` command and enabling `PROACTIVE` for `EvaluationModes` or using the PutConfigRule action and enabling `PROACTIVE` for `EvaluationModes`.

After you have turned on proactive evaluation, you can use the StartResourceEvaluation API and GetResourceEvaluationSummary API to check if the resources you specify in these commands would be flagged as NON_COMPLIANT by the proactive rules in your account in your Region.

For example, start with the StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

You should receive the `ResourceEvaluationId` in the output:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Then, use the `ResourceEvaluationId` with the GetResourceEvaluationSummary API to check the evaluation result:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

You should receive output similiar to the following:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

To see additional information about the evaluation result, such as which rule flagged a resource as NON_COMPLIANT, use the GetComplianceDetailsByResource API.

## Detective mode

Use detective evaluation to evaluate resources that have already been deployed. This allows you to evaluate the configuration settings of your existing resources.

### Evaluating your Resources (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.

2. In the AWS Management Console menu, check that the region selector is set to a Region that supports AWS Config rules. For the list of supported regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows the name, associated remediation action, and compliance status of each rule.
4. Choose a rule from the table.
5. From the **Actions** dropdown list, choose **Re-evaluate**.
6. AWS Config starts evaluating the resources against your rule.

> **Note**
>
> You can re-evaluate a rule one time each minute. You must wait for AWS Config to complete the evaluation for your rule before you start another evaluation. You can't run an evaluation if at the same time the rule is being updated or if the rule is being deleted.

### Evaluating your Resources (CLI)

- Use the **start-config-rules-evaluation** command:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config starts evaluating the recorded resource configurations against your rule. You can also specify multiple rules in your request:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

### Evaluating your Resources (API)

Use the StartConfigRulesEvaluation action.

# Deleting Evaluation Results from AWS Config Rules

After AWS Config evaluates your rule, you can see the evaluation results on the **Rules** page or the **Rules details** page for the rule. If the evaluation results are incorrect or if you want to evaluate again, you can delete the current evaluation results for the rule. For example, if your rule was incorrectly evaluating your resources or you recently deleted resources from your account, you can delete the evaluation results and then run a new evaluation.

Deleting Evaluation Results (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. In the AWS Management Console menu, verify that the Region selector is set to an AWS Region that supports AWS Config rules. For the list of supported Regions, see AWS Config Regions and Endpoints in the *Amazon Web Services General Reference*.
3. In the navigation pane, choose **Rules**. The **Rules** page shows the name, associated remediation action, and compliance status of each rule.
4. Choose a rule from the table.
5. From the **Actions** dropdown list, choose **Delete results**.
6. When prompted, type **Delete** (this entry is case sensitive), and then choose **Delete**. After you delete an evaluation, you cannot retrieve it.
7. After the evaluation results are deleted, you can manually start a new evaluation.

Deleting Evaluation Results (CLI)

- Use the **delete-evaluation-results** command.

  ```
  $ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
  ```

  AWS Config deletes the evaluation results for the rule.

Deleting Evaluation Results (API)

Use the DeleteEvaluationResults action.

# Troubleshooting for AWS Config rules

Check the following issues to troubleshoot if you cannot delete an AWS Config rule or receive an error similair to the following: "An error has occurred with AWS Config."

### The AWS Identity and Access Management (IAM) entity has permissions for the DeleteConfigRule API

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane choose **Users** or **Roles**.
3. Choose the user or role that you used to delete the AWS Config rule, and expand **Permissions policies**.
4. In the **Permissions** tab, choose **JSON**.
5. In the JSON preview pane, confirm that the IAM policy allows permissions for the DeleteConfigRule API.

### The IAM entity permission boundary allows the DeleteConfigRule API

If the IAM entity has a permissions boundary, be sure that it allows permissions for the the DeleteConfigRule API.

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane choose **Users** or **Roles**.
3. Choose the user or role that you used to delete the AWS Config rule, expand **Permissions boundary**, and then choose **JSON**.
4. In the JSON preview pane, confirm that the IAM policy allows permissions for the DeleteConfigRule API.

> **Warning**
>
> IAM users have long-term credentials, which presents a security risk. To help mitigate this risk, we recommend that you provide these users with only the permissions they require to perform the task and that you remove these users when they are no longer needed.

### The service control policy (SCP) allows the DeleteConfigRule API

1. Open the AWS Organizations console at https://console.aws.amazon.com/organizations/ using the management account for the organization.
2. In Account name, choose the AWS account.
3. In **Policies**, expand **Service control policies** and note the SCP policies that are attached.
4. At the top of the page, choose **Policies**.
5. Select the policy, and then choose **View details**.
6. In the JSON preview pane, confirm that the policy allows the DeleteConfigRule API.

### The rule is not a service-linked rule

When you enable a security standard, AWS Security Hub CSPM creates service-linked rules for you. You can't delete these service-linked rules using AWS Config, and the delete button is grayed out. To remove a service-linked rule, see Disabling a security standard in the *Security Hub CSPM User Guide*.

### No remediation actions are in progress

You cannot delete AWS Config rules that have remediation actions in progress. Follow the steps to delete the remediation action that is associated with that rule. Then, try deleting the rule again.

> **Important**
>
> Only delete remediation actions that are in **failed** or **successful** states.

# Conformance Packs for AWS Config

A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.

Conformance packs are created by authoring a YAML template that contains the list of AWS Config managed or custom rules and remediation actions. You can also use AWS Systems Manager documents (SSM documents) to store your conformance pack templates on AWS and directly deploy conformance packs using SSM document names. You can deploy the template by using the AWS Config console or the AWS CLI.

To quickly get started and to evaluate your AWS environment, use one of the sample conformance pack templates. You can also create a conformance pack YAML file from scratch based on Custom Conformance Pack.

**Topics**


- Viewing Compliance Data in the Conformance Packs Dashboard for AWS Config
- Prerequisite for Conformance Packs for AWS Config
- Region Support
- AWS Config Process Checks Within a Conformance Pack for AWS Config
- Conformance Pack Sample Templates for AWS Config
- Creating templates for Custom Conformance Packs for AWS Config
- Deploying Conformance Packs for AWS Config
- Editing Conformance Packs for AWS Config
- Deleting Conformance Packs for AWS Config
- Viewing Details and Compliance Information for your Conformance Packs for AWS Config
- Viewing the Compliance History Timeline for Conformance Packs for AWS Config
- Querying Compliance History for Conformance Packs for AWS Config
- Managing Conformance Packs for AWS Config Across all Accounts in Your Organization
- Troubleshooting for Conformance Packs for AWS Config

# Viewing Compliance Data in the Conformance Packs Dashboard for AWS Config

The main page for **Conformance Packs** displays all of the conformance packs that you currently have in your AWS account. The page also contains the name, deployment status, and compliance score of each conformance pack. A compliance score is the percentage of the number of compliant rule-resource combinations in a conformance pack compared to the number of total possible rule-resource combinations in the conformance pack.

You can use this dashboard to understand the level of compliance of your conformance packs and use the compliance score to track remediation progress, perform comparisons across different sets of requirements, and see the impact a specific change or deployment has on a conformance pack.

## Navigating the Conformance Packs Main Page

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the **Conformance packs** page. Review your conformance packs and their compliance score. You can also do the following:

   - To add and configure a new conformance pack, choose **Deploy conformance pack**.
   - To delete a conformance pack and its data, change the configuration settings, or view additional details, such as the delivery location or parameters, choose a conformance pack and choose **Actions**.

     > **Note**
     >
     > You cannot edit a deployed conformance pack. You can modify the other selections at any time by choosing the name of the conformance pack and **Edit** in the **Actions** dropdown.

   - To view the history of compliance state changes, choose a conformance pack and choose **Conformance pack timeline**. For more information, see Viewing the Compliance History Timeline for Conformance Packs.
   - To view the deployment status, compliance score, compliance score timeline, and rules for a conformance pack in a detailed view, choose a conformance pack and choose **View**.

# Prerequisite for Conformance Packs for AWS Config

Before you deploy your conformance pack, turn on AWS Config recording.

**Topics**


- Step 1: Start AWS Config Recording (Required for all conformance packs)
- Step 2: Additional Prerequisites by Conformance Pack Type


## Step 1: Start AWS Config Recording (Required for all conformance packs)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the navigation pane.
3. To start recording, under **Recording is off**, choose **Turn on**. When prompted, choose **Continue**.

## Step 2: Additional Prerequisites by Conformance Pack Type

### A. Prerequisites for Using a Conformance Pack With Remediation

Before deploying conformance packs using sample templates with remediation, you must create appropriate resources such as automation assume role and other AWS resources based on your remediation target.

If you have an existing automation role that you are using for remediation using SSM documents, you can directly provide the ARN of that role. If you have any resources you can provide those in the template.

> **Note**
>
> When deploying a conformance pack with remediation to an organization, the management account ID of the organization needs to be specified. Otherwise, during deployment of the organizational conformance pack AWS Config replaces the management account ID with the member account ID automatically.

AWS Config does not support CloudFormation intrinsic functions for the automation execution role or the `ConfigRuleName`. You must provide the exact ARN of the role as a string, and you must use the complete rule name without intrinsic functions.

For more information about how to pass the exact ARN, see Conformance Pack Sample Templates for AWS Config. While using example templates, update your Account ID and management account ID for organization.

## B. Prerequisites for Using a Conformance Pack With One or More Custom AWS Config Rules

Before deploying a conformance pack with one or more custom AWS Config rules, create appropriate resources such as AWS Lambda function and the corresponding execution role.

If you have an existing custom AWS Config rule, you can directly provide the `ARN` of AWS Lambda function to create another instance of that custom rule as part of the pack.

If you do not have an existing custom AWS Config rule, you can create a AWS Lambda function and use the ARN of the Lambda function. For more information, see AWS Config Custom Rules.

If your AWS Lambda function is present in a different AWS account, you can create AWS Config rules with appropriate cross-account AWS Lambda function authorization. For more information, see How to Centrally Manage AWS Config Rules across Multiple AWS accounts blog post.

Same account bucket policy

For AWS Config to be able to store conformance pack artifacts, you will need to provide an Amazon S3 bucket and add the following permissions. For more information on naming your bucket, see Bucket naming rules.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSConfigConformsBucketPermissionsCheck",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
```

```
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::delivery-bucket-name"
        },
        {
            "Sid": "AWSConfigConformsBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Cross-account bucket policy

For AWS Config to be able to store conformance pack artifacts, you will need to provide an Amazon S3 bucket and add the following permissions. For more information on naming your bucket, see Bucket naming rules.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSConfigConformsBucketPermissionsCheck",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
                    "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
        },
        {
            "Sid": "AWSConfigConformsBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        },
        {
            "Sid": " AWSConfigConformsBucketReadAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                ]
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/
[optional] prefix/AWSLogs/AccountID/Config/*"
        }
    ]
```

```
}
```

> **Note**
>
> When deploying cross-account conformance packs, the name of the delivery Amazon S3 bucket should start with `awsconfigconforms`.

## C. Prerequisites for Organization Conformance Packs

Specify an automation execution role ARN for that remediation in the template if the input template has an autoremediation configuration. Ensure a role with the specified name exists in all the accounts (management and member) of an organization. You must create this role in all accounts before calling `PutOrganizationConformancePack`. You can create this role manually or using the AWS CloudFormation stack-sets to create this role in every account.

If your template uses AWS CloudFormation intrinsic function `Fn::ImportValue` to import a particular variable, then that variable must be defined as an `Export Value` in all the member accounts of that organization.

For custom AWS Config rule, see How to Centrally Manage AWS Config Rules across Multiple AWS accounts blog to setup proper permissions.

**Organization bucket policy:**

For AWS Config to be able to store conformance pack artifacts, you will need to provide an Amazon S3 bucket and add the following permissions. For more information on naming your bucket, see Bucket naming rules.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
```

```
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/
config-conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

**Note**

When deploying conformance packs to an organization, the name of the delivery Amazon S3 bucket should start with `awsconfigconforms`.

# Region Support

Conformance packs are supported in the following Regions.

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS |
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

Deploying conformance packs across member accounts in an AWS Organization is supported in the following Regions.

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS | |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS | |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS | |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS | |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS | |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS | |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS | |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS | |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS | |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS | |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS | |
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS | |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS | |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS | |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS | |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS | |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS | |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# AWS Config Process Checks Within a Conformance Pack for AWS Config

Process checks is a type of AWS Config rule that allows you to track your external and internal tasks that require verification as part of the conformance packs. These checks can be added to an existing conformance pack or a new conformance pack. You can track all compliance that includes AWS Configurations and manual checks in a single location.

With process checks, you can list the compliance of requirements and actions at a single location. These process checks help increase the coverage of compliance regimes-based conformance packs. You can further expand the conformance pack by adding new process checks that track processes and actions needing manual verification and tracking. This enables conformance pack to become the template that provides details about AWS Configurations and manual processes for a compliance regime.

You can track and manage the compliance of processes not associated with resource configuration changes within a conformance packs as process checks. For example, you can add a process check to track the PCI-DSS compliance requirement to store media backup at an offsite location. You will manually evaluate the compliance of this according to PCI-DSS guidelines, or according to your organization's guidance.

**Region availability**: Process checks with the conformance packs are available in all AWS Regions where AWS Config conformance packs are available. For more information, see Region Support.

**Topics**

- Sample Conformance Pack Template for Creating Process Checks
- Include Process Checks Within a Conformance Pack
- Change Compliance Status of a Process Check
- View and Edit the Process Check (Console)

## Sample Conformance Pack Template for Creating Process Checks

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

See two sample templates, the Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1 template and the Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2 template.

## Include Process Checks Within a Conformance Pack

1. Add a process check in the conformance pack template. Refer to Sample Conformance Pack Template for Creating Process Checks.

   ```
   Resources:
     ConfigEnabledAllRegions:
       Properties:
         ConfigRuleName: Config-Enabled-All-Regions
   ```

```
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. Enter the name for the process check.
3. Enter the description for the process check.
4. Deploy the conformance pack. For more information, see Deploying Conformance Packs for AWS Config.

## Change Compliance Status of a Process Check

You can change the compliance status of a process check using the AWS Config console, the AWS CLI, and APIs.

Change Compliance Status for Process Checks (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the AWS Config Rules page.
3. Choose the name of the process check that you specified in the template along with the identifier in the conformance pack.

   > **Note**
   >
   > All the process checks from the same conformance pack have the same suffix.

4. On the Rule details page, you cannot edit the rule but you can edit the compliance of the rule. In the Manual compliance section, choose **Edit compliance**.
5. Choose the appropriate compliance from the dropdown list.
6. (Optional) Enter a description for the compliance status.
7. Choose **Save**.

Change the Compliance Status for Process Checks (AWS CLI)

You can update the compliance of process checks within a conformance pack using the AWS Command Line Interface (AWS CLI).

To install the AWS CLI on your local machine, see Installing the AWS CLI in the *AWS CLI User Guide*.

If necessary, type `AWS Configure` to configure the AWS CLI to use an AWS Region where AWS Config conformance packs are available.

1. Open a command prompt or a terminal window.
2. Enter the following command to update the compliance of a process check where `ComplianceResourceId` is your `Account ID`, and include the name of your rule.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Press Enter to run the command.

Change the Compliance Status for Process Checks (API)

After the deployment is complete, to update the evaluations and compliance of the process checks, use the `PutExternalEvaluation` API. For more information, see PutExternalEvaluation.

## View and Edit the Process Check (Console)

You can view process checks only after a compliance state has been added to process checks. Choose the specific conformance pack to view all the process checks within that conformance pack. Here you can see a list of process checks that are in compliant and noncompliant status.

Because this is a service linked rule, you cannot edit the process check through the Rule details page.

> **Note**
>
> However, you can update the compliance of the process check by choosing **Edit Compliance** and selecting the appropriate value from Compliant, noncompliant or not applicable.

You can edit or delete a process check from the conformance pack where you added the process checks.

## Conformance Pack Sample Templates for AWS Config

Here are the conformance pack YAML templates that you see in AWS Config console. Within each conformance pack template, you can use one or more AWS Config rules and remediation actions. The AWS Config rules listed within the conformance pack can be AWS Config managed rules and/or AWS Config custom rules. You can download all the conformance pack templates from GitHub.

> **Important**
>
> Conformance packs provide a general-purpose compliance framework to help you create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. AWS conformance pack sample templates intend to help you create your own conformance packs with different or additional rules, input parameters and remediation actions that suit your environment. The sample templates, including those related to compliance standards and industry benchmarks, are not designed to ensure your compliance with a specific governance standard. They can neither replace your internal efforts nor guarantee that you will pass a compliance assessment.

> **Note**
>
> It is recommended that you review the rules available in the region where you deploy a conformance pack (List of AWS Config Managed Rules by Region Availability) and amend the template for rules not yet available in that region before deploying.

**Topics**

- AWS Control Tower Detective Guardrails Conformance Pack
- Cyber Resilience Best Practices for Amazon S3, Amazon EBS, and Amazon DynamoDB
- Operational Best Practices for ABS CCIG 2.0 Material Workloads
- Operational Best Practices for ABS CCIG 2.0 Standard Workloads
- Operational Best Practices for ACSC Essential 8
- Operational Best Practices for ACSC ISM - Part 1
- Operational Best Practices for ACSC ISM - Part 2
- Operational Best Practices for AI and ML
- Operational Best Practices for Amazon API Gateway
- Operational Best Practices for Amazon CloudWatch
- Operational Best Practices for Amazon DynamoDB
- Operational Best Practices for Amazon S3
- Operational Best Practices for APRA CPG 234
- Operational Best Practices for Asset Management
- Operational Best Practices for AWS Backup
- Operational Best Practices for AWS Identity And Access Management
- Operational Best Practices for AWS Well-Architected Framework Reliability Pillar
- Operational Best Practices for AWS Well-Architected Framework Security Pillar
- Operational Best Practices for BCP and DR
- Operational Best Practices for BNM RMiT
- Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile
- Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1
- Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2
- Operational Best Practices for CIS Critical Security Controls v8 IG1
- Operational Best Practices for CIS Critical Security Controls v8 IG2
- Operational Best Practices for CIS Critical Security Controls v8 IG3
- Operational Best Practices for CIS Top 20
- Operational Best Practices for CISA Cyber Essentials
- Operational Best Practices for Criminal Justice Information Services (CJIS)

- Operational Best Practices for CMMC 2.0 Level 1
- Operational Best Practices for CMMC 2.0 Level 2
- Operational Best Practices for Compute Services
- Operational Best Practices for Data Resiliency
- Operational Best Practices for Databases Services
- Operational Best Practices for Data Lakes and Analytics Services
- Operational Best Practices for DevOps
- Operational Best Practices for EC2
- Operational Best Practices for Encryption and Key Management
- Operational Best Practices for ENISA Cybersecurity guide for SMEs
- Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low
- Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium
- Operational Best Practices for Esquema Nacional de Seguridad (ENS) High
- Operational Best Practices for FDA Title 21 CFR Part 11
- Operational Best Practices for FedRAMP(Low)
- Operational Best Practices for FedRAMP(Moderate)
- Operational Best Practices for FedRAMP (High Part 1)
- Operational Best Practices for FedRAMP (High Part 2)
- Operational Best Practices for FFIEC
- Operational Best Practices for Germany Cloud Computing Compliance Criteria Catalog (C5)
- Operational Best Practices for Gramm Leach Bliley Act (GLBA)
- Operational Best Practices for GxP EU Annex 11
- Operational Best Practices for HIPAA Security
- Operational Best Practices for IRS 1075
- Operational Best Practices for K-ISMS
- Operational Best Practices for Load Balancing
- Operational Best Practices for Logging
- Operational Best Practices for Management and Governance Services
- Operational Best Practices for MAS Notice 655
- Operational Best Practices for MAS TRMG

- Operational Best Practices for Monitoring
- Operational Best Practices for NBC TRMG
- Operational Best Practices for NERC CIP BCSI
- Operational Best Practices for NCSC Cloud Security Principles
- Operational Best Practices for NCSC Cyber Assesment Framework
- Operational Best Practices for Networking and Content Delivery Services
- Operational Best Practices for NIST 800-53 rev 4
- Operational Best Practices for NIST 800-53 rev 5
- Operational Best Practices for NIST 800 171
- Operational Best Practices for NIST 800 172
- Operational Best Practices for NIST 800 181
- Operational Best Practices for NIST 1800 25
- Operational Best Practices for NIST CSF
- Operational Best Practices for NIST Privacy Framework v1.0
- Operational Best Practices for NYDFS 23
- Operational Best Practices for NZISM 3.8
- Operational Best Practices for PCI DSS 3.2.1
- Operational Best Practices for PCI DSS 4.0 (Excluding global resource types)
- Operational Best Practices for PCI DSS 4.0 (Including global resource types)
- Operational Best Practices for Publicly Accessible Resources
- Operational Best Practices for RBI Cyber Security Framework for UCBs
- Operational Best Practices for RBI MD-ITF
- Operational Best Practices for Security, Identity, and Compliance Services
- Operational Best Practices for Serverless
- Operational Best Practices for Storage Services
- Operational Best Practices for SWIFT CSP
- Security Best Practices for Amazon Elastic Container Service (Amazon ECS)
- Security Best Practices for Amazon Elastic File System (Amazon EFS)
- Security Best Practices for Amazon Elastic Kubernetes Service (Amazon EKS)
- Security Best Practices for Amazon CloudFront

- Security Best Practices for Amazon OpenSearch Service
- Security Best Practices for Amazon Redshift
- Security Best Practices for Amazon Relational Database Service (Amazon RDS)
- Security Best Practices for AWS Auto Scaling
- Security Best Practices for AWS CloudTrail
- Security Best Practices for AWS CodeBuild
- Security Best Practices for Amazon ECR
- Security Best Practices for AWS Lambda
- Security Best Practices for AWS Network Firewall
- Security Best Practices for Amazon SageMaker AI
- Security Best Practices for AWS Secrets Manager
- Security Best Practices for AWS WAF
- Example Templates with Remediation Action

## AWS Control Tower Detective Guardrails Conformance Pack

This conformance pack contains AWS Config rules based on AWS Control Tower Detective Guardrails. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: AWS Control Tower Detective Guardrails Conformance Pack.

## Cyber Resilience Best Practices for Amazon S3, Amazon EBS, and Amazon DynamoDB

This conformance pack contains AWS Config rules based on Cyber Resilience Best Practices for Amazon S3, Amazon EBS, and Amazon DynamoDB. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Cyber Resilience Best Practices for Amazon S3, Amazon EBS, and Amazon DynamoDB.

## Operational Best Practices for ABS CCIG 2.0 Material Workloads

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the ABS Cloud Computing Implementation Guide 2.0 - Material Workloads and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ABS Cloud Computing Implementation Guide controls. An ABS Cloud Computing Implementation Guide control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-2-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4a-govern-the-cloud-2-material-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4a-govern-the-cloud-2-standard-workloads | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant . The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| section4a-govern-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| section4a-govern-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applicati ons within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| section4a-govern-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-3-material-workloads | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughpu t capacity is checked on your Amazon DynamoDB tables. This is the amount of read/ write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approache s the maximum limit for a customer's account. This rule allows you to optionall y set accountRCUThreshol dPercentage (Config Default: 80) and accountWCUThreshol dPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |
| section4a-govern-the-cloud-3-material-workloads | lambda-concurrency-check | This rule ensures that a Lambda function's concurren cy high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-3-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| section4a-govern-the-cloud-3-standard-workloads | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-3-standard-workloads | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| section4a-govern-the-cloud-3-standard-workloads | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| section4a-govern-the-cloud-3-standard-workloads | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitorin g for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| section4b-design-and-secure-the-cloud-2-standard-workloads | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-material-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| section4b-design-and-secure-the-cloud-3-material-workloads | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-material-workloads | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| section4b-design-and-secure-the-cloud-3-material-workloads | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-material-workloads | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-material-workloads | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-material-workloads | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| section4b-design-and-secure-the-cloud-3-standard-workloads | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| section4b-design-and-secure-the-cloud-3-standard-workloads | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| section4b-design-and-secure-the-cloud-4-material-workloads | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| section4b-design-and-secure-the-cloud-4-material-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| section4b-design-and-secure-the-cloud-4-material-workloads | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-4-material-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-4-material-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-4-material-workloads | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| section4b-design-and-secure-the-cloud-4-material-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-4-material-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-4-material-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-4-material-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| section4b-design-and-secure-the-cloud-4-material-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| section4b-design-and-secure-the-cloud-4-material-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-material-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| section4b-design-and-secure-the-cloud-4-standard-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-5-material-workloads | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |
| section4b-design-and-secure-the-cloud-5-material-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-material-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-5-material-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-material-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-5-standard-workloads | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-5-standard-workloads | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| section4b-design-and-secure-the-cloud-6-material-workloads | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-6-material-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-material-workloads | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-material-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-8-material-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-material-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-8-material-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-material-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-material-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| section4b-design-and-secure-the-cloud-9-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4b-design-and-secure-the-cloud-9-material-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-material-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-9-material-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-material-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-9-material-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4b-design-and-secure-the-cloud-10-material-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| section4b-design-and-secure-the-cloud-10-material-workloads | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| section4b-design-and-secure-the-cloud-10-material-workloads | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-10-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-10-material-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-10-material-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| section4b-design-and-secure-the-cloud-10-material-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-10-material-workloads | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-10-material-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-10-material-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-10-material-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| section4b-design-and-secure-the-cloud-10-material-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-10-material-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-10-material-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| section4b-design-and-secure-the-cloud-10-material-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| section4b-design-and-secure-the-cloud-10-material-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-material-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-11-material-workloads | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| section4b-design-and-secure-the-cloud-11-material-workloads | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| section4b-design-and-secure-the-cloud-11-material-workloads | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4b-design-and-secure-the-cloud-11-material-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| section4b-design-and-secure-the-cloud-11-material-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| section4b-design-and-secure-the-cloud-11-material-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-11-material-workloads | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| section4b-design-and-secure-the-cloud-11-material-workloads | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| section4b-design-and-secure-the-cloud-12-standard-workloads | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| section4b-design-and-secure-the-cloud-12-standard-workloads | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| section4b-design-and-secure-the-cloud-14-material-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| section4b-design-and-secure-the-cloud-14-material-workloads | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| section4b-design-and-secure-the-cloud-14-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | rds-in-backup-plan | To help with data backup processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| section4b-design-and-secure-the-cloud-14-material-workloads | redshift-backup-enabled | To help with data backup processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-material-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| section4b-design-and-secure-the-cloud-15-material-workloads | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-material-workloads | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| section4b-design-and-secure-the-cloud-15-material-workloads | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-material-workloads | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| section4b-design-and-secure-the-cloud-15-standard-workloads | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-1-standard-workloads | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| section4c-run-the-cloud-2-material-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-material-workloads | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| section4c-run-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4c-run-the-cloud-2-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4c-run-the-cloud-2-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4c-run-the-cloud-2-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| section4c-run-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4c-run-the-cloud-3-standard-workloads | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| section4c-run-the-cloud-3-standard-workloads | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| section4c-run-the-cloud-3-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| section4c-run-the-cloud-3-standard-workloads | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| section4c-run-the-cloud-3-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| section4c-run-the-cloud-3-standard-workloads | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| section4c-run-the-cloud-4-standard-workloads | response-plan-exists-maintained (process check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-4-material-workloads | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| section4c-run-the-cloud-4-material-workloads | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| section4c-run-the-cloud-4-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-4-material-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4c-run-the-cloud-5-standard-workloads | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |
| section4c-run-the-cloud-5-standard-workloads | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| section4c-run-the-cloud-5-standard-workloads | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| section4c-run-the-cloud-6-material-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-6-material-workloads | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| section4c-run-the-cloud-6-material-workloads | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-6-material-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4c-run-the-cloud-6-material-workloads | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-6-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| section4c-run-the-cloud-6-standard-workloads | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-6-standard-workloads | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| section4c-run-the-cloud-6-standard-workloads | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

### Template

The template is available on GitHub: Operational Best Practices for ABS CCIG 2.0 Material Workloads.

## Operational Best Practices for ABS CCIG 2.0 Standard Workloads

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the ABS Cloud Computing Implementation Guide 2.0 - Standard Workloads and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ABS Cloud Computing Implementation Guide controls. An ABS Cloud Computing Implementation Guide control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant . The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | information that accessed an Amazon S3 bucket, IP address, and time of event. |
| section4a-govern-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| section4a-govern-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| section4a-govern-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applicati ons within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| section4a-govern-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4a-govern-the-cloud-3-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-3-standard-workloads | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organizat ion's standards. |
| section4a-govern-the-cloud-3-standard-workloads | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| section4a-govern-the-cloud-3-standard-workloads | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4a-govern-the-cloud-3-standard-workloads | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-1-standard-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| section4b-design-and-secure-the-cloud-1-standard-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-2-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-2-standard-workloads | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| section4b-design-and-secure-the-cloud-2-standard-workloads | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |
| section4b-design-and-secure-the-cloud-3-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| section4b-design-and-secure-the-cloud-3-standard-workloads | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-3-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| section4b-design-and-secure-the-cloud-4-standard-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| section4b-design-and-secure-the-cloud-4-standard-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-4-standard-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-5-standard-workloads | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-5-standard-workloads | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-5-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-5-standard-workloads | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-6-standard-workloads | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| section4b-design-and-secure-the-cloud-6-standard-workloads | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-8-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-9-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-9-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| section4b-design-and-secure-the-cloud-10-standard-workloads | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-10-standard-workloads | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| section4b-design-and-secure-the-cloud-12-standard-workloads | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| section4b-design-and-secure-the-cloud-12-standard-workloads | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-12-standard-workloads | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-14-standard-workloads | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| section4b-design-and-secure-the-cloud-14-standard-workloads | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| section4b-design-and-secure-the-cloud-15-standard-workloads | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-1-standard-workloads | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| section4c-run-the-cloud-2-standard-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| section4c-run-the-cloud-2-standard-workloads | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| section4c-run-the-cloud-2-standard-workloads | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| section4c-run-the-cloud-2-standard-workloads | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-2-standard-workloads | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| section4c-run-the-cloud-2-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| section4c-run-the-cloud-3-standard-workloads | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| section4c-run-the-cloud-3-standard-workloads | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| section4c-run-the-cloud-3-standard-workloads | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| section4c-run-the-cloud-3-standard-workloads | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| section4c-run-the-cloud-3-standard-workloads | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| section4c-run-the-cloud-3-standard-workloads | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| section4c-run-the-cloud-3-standard-workloads | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| section4c-run-the-cloud-3-standard-workloads | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-3-standard-workloads | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| section4c-run-the-cloud-4-standard-workloads | response-plan-exists-maintained (process check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel. |
| section4c-run-the-cloud-5-standard-workloads | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |
| section4c-run-the-cloud-5-standard-workloads | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| section4c-run-the-cloud-5-standard-workloads | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-5-standard-workloads | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| section4c-run-the-cloud-6-standard-workloads | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-6-standard-workloads | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| section4c-run-the-cloud-6-standard-workloads | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| section4c-run-the-cloud-6-standard-workloads | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

### Template

The template is available on GitHub: Operational Best Practices for ABS CCIG 2.0 Standard Workloads.

## Operational Best Practices for ACSC Essential 8

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ACSC Essential Eight controls. An ACSC Essential Eight control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings. Some of the mappings to config rules are for the higher order section (eg. Mitigation Strategies to Limit the Extent of Cyber Security Incidents) as opposed to the more prescriptive sections.

This sample conformance pack template contains mappings to controls within the ACSC Essential 8, which was created by the Commonwealth of Australia and can be found at ACSC | Essential

Eight. Licensing of the framework under Creative Commons Attribution 4.0 International Public License and copyright information for the framework (including a disclaimer of warranties) can be found at ACSC | Copyright.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Application_control | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| Application_control | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| Application_control | cloudwatch-log-group-encryp ted | Checks if Amazon CloudWatc h Log Groups are encrypted with any AWS KMS key or a specified AWS KMS key Id. The rule is NON_COMPLIANT if a CloudWatch Log Group is |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | not encrypted with a KMS key or is encrypted with a KMS key not supplied in the rule parameter. |
| Application_control | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| Application_control | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no conditions could result in unintended behavior. |
| Application_control | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Application_control | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collection of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| Application_control | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Patch_applications | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| Patch_applications | ec2-instance-managed-by-sys tems-manager | An inventory of the software platforms and applicati ons within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Patch_applications | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |
| Patch_applications | ec2-instance-launched-with-allowed-ami | Checks if running or stopped EC2 instances were launched with Amazon Machine Images (AMIs) that meet your Allowed AMIs criteria. The rule is NON_COMPLIANT if an AMI doesn't meet the Allowed AMIs criteria and the Allowed AMIs settings isn't disabled. |
| Patch_applications | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environme nt ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Patch_applications | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| Patch_applications | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Patch_applications | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| Restrict_administrative_privileges | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Restrict_administrative_privileges | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Restrict_administrative_privileges | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Restrict_administrative_privileges | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |
| Restrict_administrative_privileges | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |
| Restrict_administrative_privileges | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Restrict_administrative_privileges | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| Restrict_administrative_privileges | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege , ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |
| Restrict_administrative_privileges | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Restrict_administrative_privileges | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |
| Restrict_administrative_privileges | rds-instance-iam-authentication-enabled | Ensure an AWS Identity and Access Management (IAM) authentication is enabled on Amazon Relational Database Service (Amazon RDS) instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). You are not required to store user credentials in the database, as authentication is managed externally. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Restrict_administrative_privileges | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| Restrict_administrative_privileges | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Restrict_administrative_privileges | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Restrict_administrative_privileges | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| Restrict_administrative_privileges | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Patch_operating_systems | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organizat ion's policies and procedures. |
| Multi-factor_authentication | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| Multi-factor_authentication | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Multi-factor_authentication | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| Multi-factor_authentication | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Multi-factor_authentication | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Regular_backups | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Regular_backups | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Regular_backups | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Regular_backups | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Regular_backups | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Regular_backups | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Regular_backups | s3-bucket-default-lock-enabled | Checks if the S3 bucket has lock enabled, by default. The rule is NON_COMPLIANT if the lock is not enabled. |
| Regular_backups | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Regular_backups | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| Regular_backups | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Regular_backups | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |
| Regular_backups | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Regular_backups | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |
| Regular_backups | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

## Template

The template is available on GitHub: Operational Best Practices for ACSC Essential 8.

# Operational Best Practices for ACSC ISM - Part 1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) 2020-06 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ISM controls. An ISM control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the ISM framework, which was created by the Commonwealth of Australia and can be found at Australian Government Information Security Manual. Licensing of the framework under Creative Commons Attribution 4.0 International Public License and copyright information for the framework (including a disclaimer of warranties) can be found at ACSC | Copyright.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 43 | response-plan-exists-maintained (process check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel. |
| 252 | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 261 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 261 | elb-logging-enabled | ELB (ELB) activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 261 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 298 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organizat ion's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 298 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 298 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 298 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (Amazon RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| 380 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |
| 459 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 459 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 459 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 459 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (Amazon EFS). |
| 459 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 459 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 459 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 459 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service(AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 459 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 459 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 459 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 459 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service(AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 459 | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 459 | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| 459 | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |
| 459 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 459 | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 459 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| 459 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| 459 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 580 | audit-log-policy-exists (process check) | Establish and maintain an audit log management policy that defines your organizat ion's logging requireme nts. This includes, but is not limited to, review and retention of audit logs. |
| 634 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 859 | cw-loggroup-retention-perio d-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 974 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 974 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management(IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1139 | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1173 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 1173 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1173 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 1173 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1173 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 1228 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1240 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| 1240 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| 1271 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1271 | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 1277 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 1277 | rds-instance-iam-authentication-enabled | Ensure an AWS Identity and Access Management (IAM) authentication is enabled on Amazon Relational Database Service (Amazon RDS) instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). You are not required to store user credentials in the database, as authentication is managed externally. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1277 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 1380 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 1380 | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatically for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 1380 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 1380 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 1380 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |
| 1380 | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |
| 1380 | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| 1380 | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |
| 1380 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | rds-instance-iam-authentication-enabled | Ensure an AWS Identity and Access Management (IAM) authentication is enabled on Amazon Relational Database Service (Amazon RDS) instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). You are not required to store user credentials in the database, as authentication is managed externally. |
| 1380 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 1380 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1380 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| 1380 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1388 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| 1388 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1401 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 1401 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1401 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 1401 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1401 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1402 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 1404 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| 1405 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1405 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 1405 | multi-region-cloudtrail-enabled | MULTI_REGION_CLOUD_TRAIL_ENABLED |
| 1405 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1405 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1405 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 1405 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1405 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 1405 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1405 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 1405 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1405 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 1405 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1405 | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |
| 1405 | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| 1405 | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1405 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1490 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| 1490 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1490 | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no conditions could result in unintended behavior. |
| 1490 | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |
| 1490 | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collection of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| 1490 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1501 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organizat ion's policies and procedures. |
| 1504 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 1504 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1504 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 1504 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1504 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 1509 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 1509 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1509 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| 1509 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1509 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1509 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 1509 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1509 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 1509 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1509 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 1509 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1509 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 1509 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1509 | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |
| 1509 | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| 1509 | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1509 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1511 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 1511 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 1511 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 1511 | rds-in-backup-plan | To help with data backup processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| 1511 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |
| 1511 | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 1511 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1511 | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |
| 1511 | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1515 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| 1515 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1515 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 1515 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1515 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 1515 | rds-in-backup-plan | To help with data backup processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1515 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 1515 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1515 | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1515 | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |
| 1515 | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1515 | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |
| 1515 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1536 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 1537 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1537 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 1552 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1552 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 1552 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 1552 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1552 | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 1579 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1580 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1580 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1580 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |
| 1650 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 1650 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| 1650 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1650 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 1650 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 1650 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 1650 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |
| 1650 | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| 1650 | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1650 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1657 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| 1657 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1657 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 1657 | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no conditions could result in unintended behavior. |
| 1657 | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1657 | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collection of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| 1657 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 1661 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1661 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 1661 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1661 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| 1661 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1661 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1661 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 1661 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1661 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1661 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 1661 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1661 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 1661 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1661 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 1679 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 1679 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1679 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 1679 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1679 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 1680 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1680 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 1680 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1680 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 1680 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1681 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 1681 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1681 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 1681 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1681 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 1683 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1683 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 1690 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1690 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 1690 | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatically for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1690 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 1690 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1690 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1690 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 1691 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1691 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 1691 | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatically for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1691 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 1691 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1691 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1691 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 1693 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1693 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 1693 | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatically for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1693 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 1693 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1693 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1693 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 1694 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1695 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 1707 | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |
| P1 | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P1 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| P3 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P5 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| P7 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P7 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| P7 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| P7 | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P8 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| P9 | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P9 | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |
| P9 | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P9 | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |
| P9 | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredR etentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P9 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| P9 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P9 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| P9 | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P9 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| P9 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P9 | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| P9 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P9 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| P10 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P10 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P10 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P10 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| P10 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| P11 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

### Template

These templates are available on GitHub:

- Operational Best Practices for ACSC ISM - Part 1
- Operational Best Practices for ACSC ISM - Part 2

## Operational Best Practices for ACSC ISM - Part 2

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides additional sample mapping between the Australian Cyber Security Centre (ACSC) Information Security Manual (ISM) 2020-06 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ISM controls. An ISM control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the ISM framework, which was created by the Commonwealth of Australia and can be found at Australian Government Information Security Manual. Licensing of the framework under Creative Commons Attribution 4.0 International Public License and copyright information for the framework (including a disclaimer of warranties) can be found at ACSC | Copyright.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1984 | appmesh-virtual-gateway-backend-defaults-tls | Checks if backend defaults for AWS App Mesh virtual gateways require the virtual gateways to communicate with all ports using TLS. The rule is NON_COMPLIANT if configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce is false. |
| 1984 | appmesh-virtual-node-backend-defaults-tls-on | Checks if backend defaults for AWS App Mesh virtual nodes require the virtual nodes to communicate with all ports using TLS. The rule is NON_COMPLIANT if configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce is false. |
| 1984 | msk-in-cluster-node-require-tls | Checks if an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1984 | rds-mysql-instance-encrypted-in-transit | Checks if connections to Amazon RDS for MySQL database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the associated database parameter group is not in-sync or if the require_secure_transport parameter is not set to 1. |
| 1984 | rds-postgres-instance-encrypted-in-transit | Checks if connections to Amazon RDS for PostgreSQL database instances are configured to use encryption in transit. The rule is NON_COMPLIANT if the associated database parameter group is not in-sync or if the rds.force_ssl parameter is not set to 1. |
| 1985 | ebs-snapshot-public-restorable-check | Checks if Amazon Elastic Block Store (Amazon EBS) snapshots are not publicly restorable. The rule is NON_COMPLIANT if one or more snapshots with RestorableByUserIds field are set to all, that is, Amazon EBS snapshots are public. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1985 | s3-bucket-mfa-delete-enabled | Checks if Amazon Elastic Block Store (Amazon EBS) snapshots are not publicly restorable. The rule is NON_COMPLIANT if one or more snapshots with RestorableByUserIds field are set to all, that is, Amazon EBS snapshots are public. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1985 | s3-bucket-public-read-prohibited | Checks if your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).<br><br>The rule is compliant when both of the following are true:<br><br>• The Block Public Access setting restricts public policies or the bucket policy does not allow public read access.<br>• The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public read access.<br><br>The rule is non-compliant when:<br><br>• If the Block Public Access setting does not restrict public policies, AWS Config evaluates whether the policy allows public read access. If the policy allows public read access, the rule is non-compliant.<br>• If the Block Public Access setting does not restrict |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | public bucket ACLs, AWS Config evaluates whether the bucket ACL allows public read access. If the bucket ACL allows public read access, the rule is non-compliant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1985 | s3-bucket-public-write-prohibited | Checks if your Amazon S3 buckets do not allow public write access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).<br><br>The rule is compliant when both of the following are true:<br><br>• The Block Public Access setting restricts public policies or the bucket policy does not allow public write access.<br>• The Block Public Access setting restricts public ACLs or the bucket ACL does not allow public write access.<br><br>The rule is non-compliant when:<br><br>• If the Block Public Access setting does not restrict public policies, AWS Config evaluates whether the policy allows public write access. If the policy allows public write access, the rule is non-compliant.<br>• If the Block Public Access setting does not restrict |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | public bucket ACLs, AWS Config evaluates whether the bucket ACL allows public write access. If the bucket ACL allows public write access, the rule is non-compliant. |
| 1985 | aurora-resources-in-logically-air-gapped-vault | Checks if Amazon Aurora DB clusters are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon Aurora DB cluster is not in a logically air-gappe d vault within the specified time period. |
| 1985 | ebs-resources-in-logically-air-gapped-vault | Checks if Amazon Elastic Block Store (Amazon EBS) volumes are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon EBS volume is not in a logically air-gapped vault within the specified time period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1985 | ec2-resources-in-logically-air-gapped-vault | Checks if Amazon Elastic Block Store (Amazon EBS) instances are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon EBS instance is not in a logically air-gapped vault within the specified time period. |
| 1985 | efs-resources-in-logically-air-gapped-vault | Checks if Amazon Elastic File System (Amazon EFS) File Systems are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon EFS File System is not in a logically air-gappe d vault within the specified time period. |
| 1985 | s3-resources-in-logically-air-gapped-vault | Checks if Amazon Simple Storage Service (Amazon S3) buckets are in a logically air-gapped vault. The rule is NON_COMPLIANT if an Amazon S3 bucket is not in a logically air-gapped vault within the specified time period. |

## Template

This templates is available on GitHub: Operational Best Practices for ACSC ISM - Part 2.

## Operational Best Practices for AI and ML

This conformance pack contains AWS Config rules based on AI and ML. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for AI and ML.

## Operational Best Practices for Amazon API Gateway

This conformance pack contains AWS Config rules based on the usage of Amazon API Gateway within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Amazon API Gateway.

## Operational Best Practices for Amazon CloudWatch

This conformance pack contains AWS Config rules based on the usage of Amazon CloudWatch within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Amazon CloudWatch.

## Operational Best Practices for Amazon DynamoDB

The template is available on GitHub: Operational Best Practices for Amazon DynamoDB.

## Operational Best Practices for Amazon S3

The template is available on GitHub: Operational Best Practices for Amazon S3.

# Operational Best Practices for APRA CPG 234

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Australian Prudential Regulation Authority (APRA) CPG 234 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more APRA CPG 234 controls. An APRA CPG 234 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within APRA CPG 234 2019, which was created by the Commonwealth of Australia and can be found at Prudential Practice Guide: CPG 234 Information Security. Licensing of the framework under Creative Commons Australia Attribution 3.0 Licence and copyright information for the framework (including a disclaimer of warranties) can be found at APRA | Copyright.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36a | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | and other details about your environment. |
| 36a | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 36a | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36b | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 36b | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36b | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 36b | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36b | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 36b | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36b | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| 36c | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36c | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 36c | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36c | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| 36c | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36c | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 36c | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 36c | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36c | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| 36d | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 36d | ebs-snapshot-public-restora ble-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 36d | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 36d | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 36d | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 36d | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 36d | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 36d | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 36d | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 36d | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 36d | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authoriza tions, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 36d | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 36d | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| 36d | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 36d | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| 36d | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| 36d | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 36d | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| 36d | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 36d | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| 36d | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 36d | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36d | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 36d | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| 36e | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| 36e | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 36e | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 36e | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 36e | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 36e | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 36e | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 36e | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 36e | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 36e | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 36e | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestric ted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 36e | s3-bucket-level-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 36e | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 36e | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 36e | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 36e | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36e | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| 36f | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 36f | ebs-snapshot-public-restora ble-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 36f | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 36f | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 36f | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 36f | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 36f | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 36f | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 36f | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 36f | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| 36f | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 36f | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestric ted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 36f | s3-bucket-level-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 36f | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 36f | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 36f | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 36f | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36f | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| 36g | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36g | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 36g | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36h | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 36h | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36h | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |
| 36h | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36h | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 36h | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36h | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 36h | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36i | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36i | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36i | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughpu t capacity is checked on your Amazon DynamoDB tables. This is the amount of read/ write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approache s the maximum limit for a customer's account. This rule allows you to optionall y set accountRCUThreshol dPercentage (Config Default: 80) and accountWCUThreshol dPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |
| 36i | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36i | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| 36i | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |
| 36i | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36i | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 36i | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36i | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| 36i | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36j | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 36j | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36j | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |
| 36j | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36j | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36j | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36j | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughpu t capacity is checked on your Amazon DynamoDB tables. This is the amount of read/ write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approache s the maximum limit for a customer's account. This rule allows you to optionall y set accountRCUThreshol dPercentage (Config Default: 80) and accountWCUThreshol dPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |
| 36j | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notificat ion Service (Amazon SNS) when a function has failed. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36j | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |
| 36j | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36j | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 36l | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| 36l | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 36l | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 36l | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 36l | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 36l | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 36l | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 36l | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 36l | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 39(a)(b)(d) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 39(a)(b)(d) | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 39(a)(b)(d) | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 40 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 40 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 40 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 40 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| 44a | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 44a | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 44a | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 44b | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 44b | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| 44b | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 44c | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| 44c | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 44c | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 44c | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 45 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 45 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 45 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| 45 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 45 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| 45 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 45 | ebs-snapshot-public-restora ble-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 45 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 45 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 45 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 45 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 45 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| 45 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 45 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 45 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 45 | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant . The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| 45 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 45 | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 45 | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| 45 | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 45 | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 45 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 45 | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 47c | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 47c | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 47c | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 47c | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 47c | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 47c | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| 47c | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 52c | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 52c | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52c | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 52c | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 52c | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 52c | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52c | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| 52c | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52c | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 52c | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 52c | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52c | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| 52c | ec2-ebs-encryption-by-defau lt | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 52c | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52c | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| 52c | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 52c | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| 52c | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 52d | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 52d | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 52d | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 52d | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| 52d | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 52d | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 52d | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 52d | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 52d | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| 52d | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 52d | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 52d | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52d | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 52e | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 52e | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 53 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 53 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthori zed users. |
| 53 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 53 | ebs-snapshot-public-restora ble-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 53 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 53 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 53 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 53 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 53 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 53 | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 53 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| 53 | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 53 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 53 | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 54 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 54 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 54 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 54 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 54 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 54 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 54 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 54 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| 54 | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 54 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 54 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 54 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 54 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| 54 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 54 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 54 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 54 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 54 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 54 | elbv2-acm-certificate-requi red | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 55 | elasticsearch-node-to-node- encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 55 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 67 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 67 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 67 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 67 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 67 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 67 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| 67 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 67 | opensearch-logs-to-cloudwat ch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 67 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 67 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 67 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 68 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 68 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 73 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 73 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(b)(h) | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(b)(h) | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AttachmentA_1(b)(h) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(b)(h) | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authoriza tions, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AttachmentA_1(b)(h) | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(b)(h) | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(b)(h) | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(b)(h) | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| AttachmentA_1(b)(h) | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(b)(h) | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AttachmentA_1(c) | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| AttachmentA_1(c) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(e) | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| AttachmentA_1(e) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(e) | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| AttachmentA_1(e) | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| AttachmentA_1(e) | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(e) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AttachmentA_1(e) | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AttachmentA_1(e) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(e) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(e) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| AttachmentA_1(e) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(e) | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| AttachmentA_1(e) | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentA_1(e) | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AttachmentA_1(e) | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AttachmentB_1 | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organizat ion from various security breaches or incidents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| AttachmentC_4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AttachmentC_4 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AttachmentC_4 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AttachmentC_4 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| AttachmentC_4 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AttachmentC_4 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AttachmentC_4 | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| AttachmentC_4 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |
| AttachmentC_4 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_4 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AttachmentC_5 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_5 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AttachmentC_5 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_5 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_5 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| AttachmentC_6 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AttachmentC_6 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_6 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| AttachmentC_7(c) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| AttachmentC_7(h) | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(h) | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AttachmentC_7(h) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AttachmentC_7(h) | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(h) | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| AttachmentC_7(h) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(h) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| AttachmentC_7(h) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(h) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| AttachmentC_7(h) | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(h) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AttachmentC_7(h) | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| AttachmentC_7(h) | opensearch-logs-to-cloudwat ch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(h) | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| AttachmentC_7(h) | elasticsearch-logs-to-cloud watch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(i) | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| AttachmentC_7(j) | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(j) | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| AttachmentC_7(j) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_7(j) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AttachmentC_8 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AttachmentC_8 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_8 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AttachmentC_8 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AttachmentC_8 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_8 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_8 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_8 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| AttachmentC_8 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_8 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| AttachmentC_8 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentC_8 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AttachmentD_1 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| AttachmentD_1 | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_4 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| AttachmentE_4 | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |
| AttachmentE_5(d) | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |
| AttachmentE_1(a)(b)(d) | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AttachmentE_1(a)(b)(d) | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| AttachmentE_1(a)(b)(d) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| AttachmentE_1(a)(b)(d) | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| AttachmentE_1(a)(b)(d) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| AttachmentE_1(a)(b)(d) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| AttachmentE_1(a)(b)(d) | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| AttachmentE_1(a)(b)(d) | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| AttachmentE_1(a)(b)(d) | kms-cmk-not-scheduled-for-d eletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| AttachmentE_1(a)(b)(d) | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AttachmentE_1(a)(b)(d) | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| AttachmentE_1(a)(b)(d) | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| AttachmentE_1(a)(b)(d) | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| AttachmentE_1(a)(b)(d) | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| AttachmentE_1(a)(b)(d) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| AttachmentE_1(a)(b)(d) | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| AttachmentE_1(a)(b)(d) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AttachmentE_1(a)(b)(d) | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| AttachmentE_1(a)(b)(d) | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

### Template

The template is available on GitHub: Operational Best Practices for APRA CPG 234.

## Operational Best Practices for Asset Management

This conformance pack contains AWS Config rules based on asset management within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Asset Management.

## Operational Best Practices for AWS Backup

This conformance pack contains AWS Config rules based on AWS Backup within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for AWS Backup.

## Operational Best Practices for AWS Identity And Access Management

The template is available on GitHub: Operational Best Practices for AWS Identity And Access Management.

## Operational Best Practices for AWS Well-Architected Framework Reliability Pillar

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Amazon Web Services' Well-Architected Framework Reliability Pillar and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more of the pillar's design principles. A Well-Architected Framework category can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-1 | How do you manage service quotas and constraints? For cloud-based | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | workload architectures, there are service quotas (which are also referred to as service limits). These quotas exist to prevent accidentally provisioning more resources than you need and to limit request rates on API operations so as to protect services from abuse. There are also resource constraints, for example, the rate that you can push bits down a fiber-optic cable, or the amount of storage on a physical disk. | | on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-1 | How do you manage service quotas and constraints? For cloud-based workload architectures, there are service quotas (which are also referred to as service limits). These quotas exist to prevent accidentally provisioning more resources than you need and to limit request rates on API operations so as to protect services from abuse. There are also resource constraints, for example, the rate that you can push bits down a fiber-optic cable, or the amount of storage on a physical disk. | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-1 | How do you manage service quotas and constraints? For cloud-based workload architectures, there are service quotas (which are also referred to as service limits). These quotas exist to prevent accidentally provisioning more resources than you need and to limit request rates on API operations so as to protect services from abuse. There are also resource constraints, for example, the rate that you can push bits down a fiber-optic cable, or the amount of storage on a physical disk. | ecs-task-definition-memory-hard-limit | Limiting the maximum memory available to your Amazon Elastic Container Service (ECS) containers ensures that your resource usage cannot be abused in the event of malicious access to your containers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-2 | How do you plan your network topology? Workloads often exist in multiple environments. These include multiple cloud environments (both publicly accessible and private) and possibly your existing data center infrastructure. Plans must include network considerations such as intra- and inter-system connectivity, public IP address management, private IP address management, and domain name resolution. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-2 | How do you plan your network topology? Workloads often exist in multiple environments. These include multiple cloud environments (both publicly accessible and private) and possibly your existing data center infrastructure. Plans must include network considerations such as intra- and inter-system connectivity, public IP address management, private IP address management, and domain name resolution. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-2 | How do you plan your network topology? Workloads often exist in multiple environments. These include multiple cloud environments (both publicly accessible and private) and possibly your existing data center infrastructure. Plans must include network considerations such as intra- and inter-system connectivity, public IP address management, private IP address management, and domain name resolution. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-5 | How do you Design Interactions in a Distributed System to Mitigate or Withstand Failures? Distributed systems rely on communications networks to interconnect components, such as servers or services. Your workload must operate reliably despite data loss or latency in these networks. Components of the distributed system must operate in a way that does not negatively impact other components or the workload. These best practices prevent failures and improve mean time between failures (MTBF). | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | beanstalk-enhanced -health-reporting- enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastru cture. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | ecs-container-insi ghts-enabled | Monitoring is an important part of maintaining the reliability, availabil ity, and performan ce of Amazon Elastic Container Service (ECS) and your AWS solutions. Container Insights also provides diagnostic informati on, such as container restart failures, to help you isolate issues and resolve them quickly. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | ec2-instance-detai led-monitoring-ena bled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitorin g on the Amazon EC2 console, which displays monitorin g graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | rds-enhanced-monit oring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availabil ity. This provides detailed visibility into the health of your Amazon RDS database instances . When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-6 | How do you monitor workload resources ? Logs and metrics are powerful tools to gain insight into the health of your workload. You can configure your workload to monitor logs and metrics and send notifications when thresholds are crossed or significa nt events occur. Monitoring enables your workload to recognize when low-performance thresholds are crossed or failures occur, so it can recover automatically in response. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-7 | How do you design your workload to adapt to changes in demand? A scalable workload provides elasticity to add or remove resources automatically so that they closely match the current demand at any given point in time. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-7 | How do you design your workload to adapt to changes in demand? A scalable workload provides elasticity to add or remove resources automatically so that they closely match the current demand at any given point in time. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-7 | How do you design your workload to adapt to changes in demand? A scalable workload provides elasticity to add or remove resources automatically so that they closely match the current demand at any given point in time. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-8 | How do you implement change? Controlled changes are necessary to deploy new functionality, and to ensure that the workloads and the operating environment are running known software and can be patched or replaced in a predictable manner. If these changes are uncontrolled, then it makes it difficult to predict the effect of these changes, or to address issues that arise because of them. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-8 | How do you implement change? Controlled changes are necessary to deploy new functiona lity, and to ensure that the workloads and the operating environment are running known software and can be patched or replaced in a predictable manner. If these changes are uncontrolled, then it makes it difficult to predict the effect of these changes, or to address issues that arise because of them. | rds-automatic-mino r-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed , which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-8 | How do you implement change? Controlled changes are necessary to deploy new functionality, and to ensure that the workloads and the operating environment are running known software and can be patched or replaced in a predictable manner. If these changes are uncontrolled, then it makes it difficult to predict the effect of these changes, or to address issues that arise because of them. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-8 | How do you implement change? Controlled changes are necessary to deploy new functionality, and to ensure that the workloads and the operating environment are running known software and can be patched or replaced in a predictable manner. If these changes are uncontrolled, then it makes it difficult to predict the effect of these changes, or to address issues that arise because of them. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-9 | How do you back up data? Back up data, applications, and configuration to meet your requirements for recovery time objectives (RTO) and recovery point objectives (RPO). | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | clb-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | lambda-vpc-multi-az-check | If your AWS Lambda function is configured to connect to a virtual private cloud (VPC) in your account, deploy the AWS Lambda function in at least two different Availability Zones to ensure that it is your function is available to process events in case of a service interruption in a single zone. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | opensearch-data-node-fault-tolerance | Amazon OpenSearch Service (OpenSearch Service) requires at least three data nodes for high availability and fault-tolerance. Deploying an OpenSearch Service domain with at least three data nodes ensures cluster operations if a node fails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| REL-10 | How do you use fault isolation to protect your workload? Fault isolated boundaries limit the effect of a failure within a workload to a limited number of components. Components outside of the boundary are unaffected by the failure. Using multiple fault isolated boundaries, you can limit the impact on your workload. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

## Template

The template is available on GitHub: Operational Best Practices for AWS Well-Architected Reliability Pillar.

# Operational Best Practices for AWS Well-Architected Framework Security Pillar

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Amazon Web Services' Well-Architected Framework Security Pillar and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more of the pillar's design principles. A Well-Architected Framework category can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-1 | How do you securely operate your workload? To operate your workload securely, you must apply overarching best practices to every area of security. Take requirements and processes that you have defined in operational excellence at an organizational and workload level, and apply them to all areas. Staying up to date with AWS and industry recommendations and threat intelligence helps you evolve your threat model and control objectives. Automating security processes, testing, and validation allow you to scale your security operations. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentia ls. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Managemen t (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentia ls. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | secretsmanager-rot ation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | secretsmanager-sch eduled-rotation-su ccess-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | secretsmanager-sec ret-periodic-rotation | This rule ensures AWS Secrets Manager secrets have periodic rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | secretsmanager-sec ret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | secretsmanager-usi ng-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-2 | How do you manage identities for people and machines? There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right condition s. Human Identitie s: Your administr ators, developers, operators, and end users require an identity to access your AWS environme nts and applications. These are members of your organizat ion, or external users with whom you collaborate, and who interact with your AWS resources from a web browser, | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | client applicati on, or interactive command-line tools. Machine Identities: Your service applicati ons, operational tools, and workloads require an identity to make requests to AWS services - for example, to read data. These identitie s include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions . You might also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-3 | How do you manage permissio ns for people and machines? Each component or resource of your workload needs to be accessed by administr ators, end users, or other components. Have a clear definitio n of who or what should have access to each component, choose the appropria te identity type and method of authentic ation and authoriza tion. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissio ns for people and machines? Each component or resource of your workload needs to be accessed by administr ators, end users, or other components. Have a clear definitio n of who or what should have access to each component, choose the appropria te identity type and method of authentic ation and authoriza tion. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-3 | How do you manage permissio ns for people and machines? Each component or resource of your workload needs to be accessed by administr ators, end users, or other components. Have a clear definitio n of who or what should have access to each component, choose the appropria te identity type and method of authentic ation and authoriza tion. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-3 | How do you manage permissions for people and machines? Establish common controls that restrict access to all identities in your organization. For example, you can restrict access to specific AWS Regions, or prevent your operators from deleting common resources, such as an IAM role used for your central security team | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |
| SEC-3 | How do you manage permissions for people and machines? Continuously monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| SEC-3 | How do you manage permissio ns for people and machines? Continuou sly monitor findings that highlight public and cross account access. Reduce public access and cross account access to only resources that require this type of access. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an object in an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-4 | How do you detect and investigate security events? Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√ ¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√ ¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√ ¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√ ¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√ ¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | ec2-instance-multi ple-eni-check | This rule checks if your Amazon Elastic Compute Cloud (Amazon EC2) instances have multiple ENIs. Having multiple ENIs can cause dual-homed instances, meaning instances that have multiple subnets. This can add network security complexit y and introduce unintended network paths and access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√ ¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectiv ity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no condition s could result in unintended behavior. |
| SEC-5 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-5 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collectio n of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| SEC-5 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | vpc-network-acl-un used-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SEC-5 | How do you protect your network resources? Any workload that has some form of network connectivity, whether it,Äö√Ñ√¥s the internet or a private network, requires multiple layers of defense to help protect from external and internal network-based threats. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed , which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | elastic-beanstalk-managed-updates-en abled | Enabling managed platform updates for an Amazon Elastic Beanstalk environme nt ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ecr-private-image-scanning-enabled | Amazon Elastic Container Repositor y (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ecs-container-insi ghts-enabled | Monitoring is an important part of maintaining the reliability, availabil ity, and performan ce of Amazon Elastic Container Service (ECS) and your AWS solutions. Container Insights also provides diagnostic informati on, such as container restart failures, to help you isolate issues and resolve them quickly. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-instance-multi ple-eni-check | This rule checks if your Amazon Elastic Compute Cloud (Amazon EC2) instances have multiple ENIs. Having multiple ENIs can cause dual-homed instances, meaning instances that have multiple subnets. This can add network security complexit y and introduce unintended network paths and access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances , containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-6 | How do you protect your compute resources? Compute resources in your workload require multiple layers of defense to help protect from external and internal threats. Compute resources include EC2 instances, containers, AWS Lambda functions, database services, IoT devices, and more. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implement ing multiple controls, to reduce the risk of unauthorized access or mishandling. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implement ing multiple controls, to reduce the risk of unauthorized access or mishandling. | s3-bucket-server-s ide-encryption-ena bled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implement ing multiple controls, to reduce the risk of unauthorized access or mishandling. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implement ing multiple controls, to reduce the risk of unauthorized access or mishandling. | account-part-of-or ganizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsist ent account configura tions, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-8 | How do you protect your data at rest? Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SEC-9 | How do you protect your data in transit? Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

### Template

The template is available on GitHub: Operational Best Practices for AWS Well-Architected Security Pillar.

## Operational Best Practices for BCP and DR

This conformance pack contains AWS Config rules based on BCP and DR within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for BCP and DR.

## Operational Best Practices for BNM RMiT

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard.

You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Bank Negara Malaysia (BNM) Risk Management in Technology (RMiT) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more BNM RMiT controls. A BNM RMiT control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Where this involves a reliance on third-party assessments, the financial institution shall consider whether such reliance is consistent with the financial institution's risk appetite and tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | api-gw-cache-enabl ed-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | cloudwatch-log-gro up-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | cmk-backing-key-ro tation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | dynamodb-table-enc rypted-kms | Ensure that encryptio n is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | kms-cmk-not-schedu led-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | opensearch-encrypt ed-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | opensearch-https-r equired | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | opensearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | rds-snapshot-encry pted | Ensure that encryptio n is enabled for your Amazon Relationa l Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | rds-storage-encryp ted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | s3-bucket-server-s ide-encryption-ena bled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | sagemaker-endpoint -configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | sagemaker-notebook -instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | secretsmanager-usi ng-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.18 | A financial instituti on must conduct due diligence and evaluate the cryptographic controls associated with the technolog y used in order to protect the confident iality, integrity , authentication, authorisation and non -repudiation of information. Where a financial instituti on does not generate its own encryption keys, the financial institution shall undertake appropria te measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third-party assessments, the financial instituti on shall consider whether such reliance is consistent with the financial instituti on's risk appetite and | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | tolerance. A financial institution must also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.20 | A financial institution shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised certificate authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/regulatory specifications. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.20 | A financial institution shall store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers shall be issued by recognised certificate authorities. The financial institution must ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the use of private cryptographic keys corresponding to the user certificates are legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates must be consistent with industry best practices and applicable legal/regulatory specifications. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.27 | A financial institution must establish real-time monitoring mechanisms to track capacity utilisation and performance of key processes and services. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.34 | A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.34 | A financial institution must ensure the network services for its critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.35 | A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies. | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. Ensure X-Ray is enables so you can see detailed information not only about the request and response, but also about calls that your application makes to downstream AWS resources, microservices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.35 | A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.35 | A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.35 | A financial institution must establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 10.36 | A financial institution must ensure network services supporting critical systems are designed and implemented to ensure the confidentiality, integrity and availability of data. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.36 | A financial institution must ensure network services supportin g critical systems are designed and implemented to ensure the confident iality, integrity and availability of data. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| 10.36 | A financial institution must ensure network services supportin g critical systems are designed and implemented to ensure the confident iality, integrity and availability of data. | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.36 | A financial institution must ensure network services supportin g critical systems are designed and implemented to ensure the confident iality, integrity and availability of data. | elb-deletion-prote ction-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |
| 10.36 | A financial institution must ensure network services supportin g critical systems are designed and implemented to ensure the confident iality, integrity and availability of data. | nlb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Network Load Balancers (NLBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.38 | A financial institution must ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial instituti on must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthori sed disclosure and access. This shall include retaining ownership, control and management of all data pertainin g to customer and counterpa rty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial instituti on must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthori sed disclosure and access. This shall include retaining ownership, control and management of all data pertainin g to customer and counterpa rty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial instituti on must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthori sed disclosure and access. This shall include retaining ownership, control and management of all data pertainin g to customer and counterpa rty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial instituti on must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthori sed disclosure and access. This shall include retaining ownership, control and management of all data pertainin g to customer and counterpa rty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial instituti on must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthori sed disclosure and access. This shall include retaining ownership, control and management of all data pertainin g to customer and counterpa rty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.51 | A financial institution must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial instituti on must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial instituti on must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.52 | A financial institution must implement an appropriate access controls policy for the identification, authentication and authorisation of users (internal and external users such as third-party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(b)(h)(i) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficien t permissions are granted to legitimat e users to perform their roles; (h) limit and control the sharing of user ID and passwords across multiple users; and (i) control the use of generic user ID naming conventio ns in favour of more personally identifia ble IDs. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(b) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficien t permissions are granted to legitimat e users to perform their roles; | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(b) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficien t permissions are granted to legitimat e users to perform their roles; | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(b) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(b) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficien t permissions are granted to legitimat e users to perform their roles; | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(b) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.53(b) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 10.53(b) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (b) employ "least privilege" access rights or on a 'need-to-have' basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles; | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(c)(f) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (c) employ time-bound access rights which restrict access to a specific period including access rights granted to service providers ; (f) adopt stronger authentication for critical activities including for remote access | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| 10.53(f)(h) | In observing paragraph 10.52, a financial institution should consider the following principles in its access control policy: (f) adopt stronger authentication for critical activities including for remote access; (h) limit and control the sharing of user ID and passwords across multiple users | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(f)(h) | In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (f) adopt stronger authentication for critical activities including for remote access; (h) limit and control the sharing of user ID and passwords across multiple users | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.53(f)(h) | In observing paragraph 10.54, a financial institution should consider the following principles in its access control policy: (f) adopt stronger authentic ation for critical activities including for remote access; (h) limit and control the sharing of user ID and passwords across multiple users | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.54 | A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (for example password, PIN), something the user possesses (for example smart card, security device) and something the user is (for example biometric characteristics, such as a fingerprint or retinal pattern). | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.54 | A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (for example password, PIN), something the user possesses (for example smart card, security device) and something the user is (for example biometric characteristics, such as a fingerprint or retinal pattern). | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a username and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.54 | A financial institution must employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall be commensurate with the criticality of the functions and adopt at least one or more of these three basic authentication factors, namely, something the user knows (for example password, PIN), something the user possesses (for example smart card, security device) and something the user is (for example biometric characteristics, such as a fingerprint or retinal pattern). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.55 | A financial instituti on shall periodically review and adapt its password practices to enhance resilienc e against evolving attacks. This includes the effective and secure generation of passwords. There must be appropriate controls in place to check the strength of the passwords created. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.56 | Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial institutions are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.56 | Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial instituti ons are encourage d to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.56 | Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, financial instituti ons are encourage d to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that are more reliable and provide stronger fraud deterrents | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial instituti on must ensure (a ) access controls to enterprise-wide systems are effective ly managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.59 | A financial institution must ensure (a) access controls to enterprise-wide systems are effectively managed and monitored; and (b) user activities in critical systems are logged for audit and investigations. Activity logs must be maintained for at least three years and regularly reviewed in a timely manner. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.60 | In fulfilling the requirement under paragraph 10.59, large financial institutions are required to (a) deploy an identity access management system to effectively manage and monitor user access to enterpris e-wide systems; and (b) deploy automated audit tools to flag any anomalies. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 10.60 | In fulfilling the requirement under paragraph 10.61, large financial institutions are required to (a) deploy an identity access management system to effectively manage and monitor user access to enterpris e-wide systems; and (b) deploy automated audit tools to flag any anomalies. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.60 | In fulfilling the requirement under paragraph 10.61, large financial institutions are required to (a) deploy an identity access management system to effectively manage and monitor user access to enterpris e-wide systems; and (b) deploy automated audit tools to flag any anomalies. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.61 | A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.61 | A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.61 | A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.61 | A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.61 | A financial institution must ensure that critical systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, a financial institution must clearly assign responsibilities to identified functions: (a) to continuously monitor and implement latest patch releases in a timely manner; and (b) identify critical technology systems that are approaching EOL for further remedial action. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| 10.64(a) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.64(a) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |
| 10.64(a) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | cloudwatch-log-gro up-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 10.64(a) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | opensearch-encrypt ed-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 10.64(a) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (a) confidentiality and integrity of customer and counterparty information and transactions | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.64(b) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| 10.64(b) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(b) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 10.64(b) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | nlb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your NetworkLoad Balancers (NLBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(b) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(b) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(b) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(b) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (b) reliability of services delivered from channels and devices with minimum disruption to services | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(d) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (d) sufficient audit trail and monitoring of anomalous transactions | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial instituti on must implement robust technolog y security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.64(e) | A financial institution must implement robust technology security controls in providing digital services which assure the following: (e) ability to identify and revert to the recovery point prior to incident or service disruption | s3-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Simple Storage Service (S3) buckets are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.7 | A financial institution must deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure. The scope of monitoring must cover all critical systems including the supporting infrastructure. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.7 | A financial institution must deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its technology infrastructure. The scope of monitoring must cover all critical systems including the supporting infrastructure. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.8 | A financial institution must ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture. For large financial institutions, this must include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.8 | A financial institution must ensure that its cybersecurity operations continuously prevent and detect any potential compromise of its security controls or weakening of its security posture. For large financial institutions, this must include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.18(c)(f) | The SOC must be able to perform the following functions : (c) vulnerability management; (f) provision of situation al awareness to detect adversaries and threats including threat intellige nce analysis and operations, and monitoring indicator s of compromise (IOC). This includes advanced behaviour al analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.18(c)(f) | The SOC must be able to perform the following functions : (c) vulnerability management; (f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC). This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.18(c)(f) | The SOC must be able to perform the following functions : (c) vulnerability management; (f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC). This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.1 | Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.1 | Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.5(b) | Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Appendix 5.5(b) | Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.5(b) | Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| Appendix 5.5(b) | Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Appendix 5.5(b) | Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Appendix 5.5(b) | Ensure security controls for server-to-server external network connections include the following: (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Appendix 5.5(c) | Ensure security controls for server-to-server external network connections include the following : (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| Appendix 5.5(c) | Ensure security controls for server-to-server external network connections include the following : (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.5(c) | Ensure security controls for server-to-server external network connections include the following : (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.6 | Ensure security controls for remote access to server include the following : (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPSec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.6 | Ensure security controls for remote access to server include the following : (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPSec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.6 | Ensure security controls for remote access to server include the following : (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPSec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.6 | Ensure security controls for remote access to server include the following : (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPSec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.6 | Ensure security controls for remote access to server include the following : (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPSec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 5.6 | Ensure security controls for remote access to server include the following : (a) restrict access to only hardened and locked down end-point devices; (b) use secure tunnels such as TLS and VPN IPSec; (c) deploy 'gateway' server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and (d) close relevant ports immediately upon expiry of remote access. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (a) | A financial institution should design a robust cloud architecture and ensure such design is in accordance with the relevant international standards for the intended application. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| Appendix 10 Part B - 1 (b) | A financial institution is encouraged to adopt zero-trust principles to provide a cyber resilient architecture by adopting an "assume breach" mindset, layering defense-in-depth through micro-segmentation, "deny-by-default", "least privilege" access rights, and conducting deep inspection and continuous validation where applicable. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (b) | A financial institution is encouraged to adopt zero-trust principles to provide a cyber resilient architecture by adopting an "assume breach" mindset, layering defense-in-depth through micro-segmentation, "deny-by-default", "least privilege" access rights, and conducting deep inspection and continuous validation where applicable. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (b) | A financial institution is encouraged to adopt zero-trust principles to provide a cyber resilient architecture by adopting an "assume breach" mindset, layering defense-in-depth through micro-segmentation, "deny-by-default", "least privilege" access rights, and conducting deep inspection and continuous validation where applicable. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (b) | A financial institution is encouraged to adopt zero-trust principles to provide a cyber resilient architecture by adopting an "assume breach" mindset, layering defense-in-depth through micro-segmentation, "deny-by-default", "least privilege" access rights, and conducting deep inspection and continuous validation where applicable. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (c) | A financial institution should use the latest network architecture approach and appropriate network design concept and solutions for managing and monitoring granular network security and centralized network provision in managing complexity of the cloud network environment. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Appendix 10 Part B - 1 (c) | A financial institution should use the latest network architecture approach and appropriate network design concept and solutions for managing and monitoring granular network security and centralized network provision in managing complexity of the cloud network environment. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (d) | A financial institution should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| Appendix 10 Part B - 1 (d) | A financial institution should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (f) i) | The increasing use of applicati on programming interfaces (API) by financial instituti on to interconn ect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface and any mismanage ment may amplify the impact of an information security incident. A financial institution should ensure its APIs are subject to rigorous management and control mechanism s which include the following: i) APIs should be designed for service resilienc e to avoid the risk of single points of failure and configure d securely with appropriate access controls; | api-gwv2-authoriza tion-type-configured | Ensure your Amazon API Gateway v2 API route has an authorization type set to prevent unauthorized access to the underlying backend resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (f) ii) | The increasing use of applicati on programming interfaces (API) by financial instituti on to interconn ect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface and any mismanage ment may amplify the impact of an information security incident. A financial institution should ensure its APIs are subject to rigorous management and control mechanism s which include the following: ii) APIs should be tracked and monitored against cyber-att acks with adequate incident response measures and are de-commissioned on a | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | timely basis when no longer in use. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 1 (f) ii) | The increasing use of applicati on programming interfaces (API) by financial instituti on to interconn ect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface and any mismanage ment may amplify the impact of an information security incident. A financial institution should ensure its APIs are subject to rigorous management and control mechanism s which include the following: ii) APIs should be tracked and monitored against cyber-att acks with adequate incident response measures and are de-commissioned on a | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | timely basis when no longer in use. | | |
| Appendix 10 Part B - 2 (b) ii) | A financial institution should continuously leverage enhanced cloud capabilities to improve the security of the cloud services and financial institutions are, among others, encouraged to: ii) use immutable infrastructure practices for deployment of services to reduce the risk of failure by creating a new environment with the latest stable version of the software. The on-going monitoring of the cloud environment should include automating the detection of changes to immutable infrastructure to improve compliance review and combat evolving cyber-attacks | cloudformation-stack-notification-check | To detect unintended changes to the underlying AWS resources, ensure your CloudFormation stack is configured to send event notifications to an Amazon SNS topic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 3 (b) vi) | A financial institution should ensure virtual machine and container images are configured, hardened, and monitored appropriately. This includes the following: vi) stored images are subjected to security monitoring from unauthorised access and changes. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (a) i) | As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following: i) define and formalise backup and recovery strategy at the planning stage of cloud adoption; | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (a) i) | As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following: i) define and formalise backup and recovery strategy at the planning stage of cloud adoption; | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (a) i) | As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following: i) define and formalise backup and recovery strategy at the planning stage of cloud adoption; | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (a) i) | As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following: i) define and formalise backup and recovery strategy at the planning stage of cloud adoption; | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (a) i) | As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following: i) define and formalise backup and recovery strategy at the planning stage of cloud adoption; | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (a) i) | As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following: i) define and formalise backup and recovery strategy at the planning stage of cloud adoption; | s3-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Simple Storage Service (S3) buckets are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (b) | A financial institution should ensure backup and restoration procedures are periodically tested to validate recovery capabilities. The frequency of backup procedures should be commensurate with the criticality of the system and recovery point objective (RPO) of the system. Remedial actions should be taken promptly by the financial institution for unsuccessful backups. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (c) i) | A financial institution should ensure sufficient backup and recovery of virtual machine and container including backup configuration settings (for IaaS and PaaS, where relevant), which includes the following: i) ensure the capability to restore a virtual machine and container at point-in-time as specified by the the business recovery objectives; | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (d) i) | A financial instituti on should assess the resilience requireme nts of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availabil ity in the extreme adverse scenarios . Financial instituti ons should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentra tion risk. Amongst the viable options are: i) leverage cloud services' high availability and redundancy features to ensure productio n data centres have redundant capacity in different availability zones; | autoscaling-multiple-az | To ensure high availability, ensure your Auto Scaling group is configure d to span multiple Availability Zones. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (d) i) | A financial instituti on should assess the resilience requireme nts of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availabil ity in the extreme adverse scenarios . Financial instituti ons should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentra tion risk. Amongst the viable options are: i) leverage cloud services' high availability and redundancy features to ensure productio n data centres have redundant capacity in different availability zones; | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, container s, and IP addresses , in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (d) i) | A financial instituti on should assess the resilience requireme nts of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availabil ity in the extreme adverse scenarios . Financial instituti ons should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentra tion risk. Amongst the viable options are: i) leverage cloud services' high availability and redundancy features to ensure productio n data centres have redundant capacity in different availability zones; | lambda-vpc-multi-az-check | If your AWS Lambda function is configure d to connect to a virtual private cloud (VPC) in your account, deploy the AWS Lambda function in at least two different Availability Zones to ensure that it is your function is available to process events in case of a service interruption in a single zone. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (d) i) | A financial instituti on should assess the resilience requireme nts of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availabil ity in the extreme adverse scenarios . Financial instituti ons should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentra tion risk. Amongst the viable options are: i) leverage cloud services' high availability and redundancy features to ensure productio n data centres have redundant capacity in different availability zones; | nlb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your NetworkLoad Balancers (NLBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (d) i) | A financial institution should assess the resilience requirements of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availability in the extreme adverse scenarios. Financial institutions should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentration risk. Amongst the viable options are: i) leverage cloud services' high availability and redundancy features to ensure production data centres have redundant capacity in different availability zones; | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 5 (d) i) | A financial instituti on should assess the resilience requireme nts of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availabil ity in the extreme adverse scenarios . Financial instituti ons should consider a risk-based approach and progressively adopt appropriate mitigating controls to ensure service availability and mitigate concentra tion risk. Amongst the viable options are: i) leverage cloud services' high availability and redundancy features to ensure productio n data centres have redundant capacity in different availability zones; | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | eks-secrets-encrypted | To help protect data at rest, ensure that your Amazon Elastic Kubernetes Service (EKS) clusters are configured to have Kubernetes secrets encrypted. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| Appendix 10 Part B - 8 (a) | A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (d) | As the usage of cloud adoption increases , managing many encryption keys used for protectin g data has become more complex and may introduce new challenges for financial institutions. A financial instituti on should adopt a comprehensive and centralized approach to key managemen t including the use of centralised key management system that can handle generations, storage and distribution of keys in a secure and scalable manner. | cmk-backing-key-ro tation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 8 (d) | As the usage of cloud adoption increases , managing many encryption keys used for protectin g data has become more complex and may introduce new challenges for financial institutions. A financial instituti on should adopt a comprehensive and centralized approach to key managemen t including the use of centralised key management system that can handle generations, storage and distribution of keys in a secure and scalable manner. | kms-cmk-not-schedu led-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) ii) | The management plane is a key security difference between traditional infrastru cture and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deploymen t. In view of this, financial Instituti ons should ensure the use of strong controls for accessing the management plane which may include the following : ii) implement "least privilege" and strong multi-factor authentication (MFA) for example, strong password, soft token, privileged access management tool and maker-checker functions; | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) ii) | The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following: ii) implement "least privilege" and strong multi-factor authentication (MFA) for example, strong password, soft token, privileged access management tool and maker-checker functions; | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) ii) | The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following: ii) implement "least privilege" and strong multi-factor authentication (MFA) for example, strong password, soft token, privileged access management tool and maker-checker functions; | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) ii) | The management plane is a key security difference between traditional infrastru cture and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deploymen t. In view of this, financial Instituti ons should ensure the use of strong controls for accessing the management plane which may include the following : ii) implement "least privilege" and strong multi-factor authentication (MFA) for example, strong password, soft token, privileged access management tool and maker-checker functions; | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) iii) | The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following: iii) employ granular entitlement allocation for privileged users; | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) iii) | The management plane is a key security difference between traditional infrastru cture and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deploymen t. In view of this, financial Instituti ons should ensure the use of strong controls for accessing the management plane which may include the following : iii) employ granular entitlement allocatio n for privileged users; | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) iv) | The management plane is a key security difference between traditional infrastru cture and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deploymen t. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following: iv) conduct continuou s monitoring of the activities performed by privileged users; | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 9 (a) iv) | The management plane is a key security difference between traditional infrastru cture and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deploymen t. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which may include the following: iv) conduct continuou s monitoring of the activities performed by privileged users; | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 12 (a) | A financial institution should protect the data hosted in cloud services as required under the Data Loss Prevention section (paragraphs 11.14 to 11.16) of this policy document, including the expansion of the endpoint footprint if the financial institution allows its staff to use their own devices to access the sensitive data. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Appendix 10 Part B - 12 (a) | A financial institution should protect the data hosted in cloud services as required under the Data Loss Prevention section (paragraphs 11.14 to 11.16) of this policy document, including the expansion of the endpoint footprint if the financial institution allows its staff to use their own devices to access the sensitive data. | macie-status-check | Amazon Macie is a data security service that uses machine learning (ML) and pattern matching to discover and help protect your sensitive data stored in Amazon Simple Storage Service (S3) buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 14 (c) i) | A financial instituti on should consider the following additional measures in the developme nt of its CIRP: i) enhance its ability to detect security breach incidents to achieve effective incident managemen t, including the ability to detect data leakage on the dark web; | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Appendix 10 Part B - 14 (c) i) | A financial institution should consider the following additional measures in the development of its CIRP: i) enhance its ability to detect security breach incidents to achieve effective incident management, including the ability to detect data leakage on the dark web; | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

### Template

The template is available on GitHub: Operational Best Practices for BNM RMiT.

## Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom

AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CCCS Medium Cloud Control Profile controls. A CCCS Medium Cloud Control Profile control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(1) | AC-2(1) Account Management \| Automated System Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(3) | AC-2(3) Account Management \| Disable Inactive Accounts | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(3) | AC-2(3) Account Management \| Disable Inactive Accounts | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) Account Management \| Automated Audit Actions | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AC-2(4) | AC-2(4) Account Management \| Automated Audit Actions | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) Account Management \| Automated Audit Actions | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) Account Management \| Automated Audit Actions | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) Account Management \| Automated Audit Actions | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-2(4) | AC-2(4) Account Management \| Automated Audit Actions | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2(4) | AC-2(4) Account Management \| Automated Audit Actions | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.A | AC-2.A Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.B | AC-2.B Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.C | AC-2.C Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.D | AC-2.D Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.E | AC-2.E Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.F | AC-2.F Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.G | AC-2.G Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.H | AC-2.H Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.I | AC-2.I Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.J | AC-2.J Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-2.K | AC-2.K Account Management | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-3.A | AC-3.A Access Enforcement | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-4(21) | AC-4(21) Information Flow Enforcement \| Physical / Logical Separation of Information Flows | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-4.A | AC-4.A Information Flow Enforcement | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A Separation of Duties | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A Separation of Duties | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A Separation of Duties | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A Separation of Duties | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-5.A | AC-5.A Separation of Duties | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(1) | AC-6(1) Least Privilege \| Authorize Access to Security Functions | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(1) | AC-6(1) Least Privilege \| Authorize Access to Security Functions | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(1) | AC-6(1) Least Privilege \| Authorize Access to Security Functions | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(1) | AC-6(1) Least Privilege \| Authorize Access to Security Functions | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(1) | AC-6(1) Least Privilege \| Authorize Access to Security Functions | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) Least Privilege \| Non-Privileged Access for Non-Security Functions | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) Least Privilege \| Non-Privileged Access for Non-Security Functions | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) Least Privilege \| Non-Privileged Access for Non-Security Functions | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) Least Privilege \| Non-Privileged Access for Non-Security Functions | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(2) | AC-6(2) Least Privilege \| Non-Privileged Access for Non-Security Functions | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(5) | AC-6(5) Least Privilege \| Privileged Accounts | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(5) | AC-6(5) Least Privilege \| Privileged Accounts | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(5) | AC-6(5) Least Privilege \| Privileged Accounts | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(5) | AC-6(5) Least Privilege \| Privileged Accounts | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CCCS-fPBMM-AC-6(9) | AC-6(9) Least Privilege \| Auditing Use of Privileged Functions | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) Least Privilege \| Auditing Use of Privileged Functions | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-AC-6(9) | AC-6(9) Least Privilege \| Auditing Use of Privileged Functions | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) Least Privilege \| Auditing Use of Privileged Functions | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) Least Privilege \| Auditing Use of Privileged Functions | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) Least Privilege \| Auditing Use of Privileged Functions | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(9) | AC-6(9) Least Privilege \| Auditing Use of Privileged Functions | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(10) | AC-6(10) Least Privilege \| Prohibit Non-Privileged Users from Executing Privileged Functions | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(10) | AC-6(10) Least Privilege \| Prohibit Non-Privileged Users from Executing Privileged Functions | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(10) | AC-6(10) Least Privilege \| Prohibit Non-Privileged Users from Executing Privileged Functions | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6(10) | AC-6(10) Least Privilege \| Prohibit Non-Privileged Users from Executing Privileged Functions | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-6(10) | AC-6(10) Least Privilege \| Prohibit Non-Privileged Users from Executing Privileged Functions | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-6.A | AC-6.A Least Privilege | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(1) | AC-17(1) Remote Access \| Automated Monitoring / Control | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(2) | AC-17(2) Remote Access \| Protection of Confidentiality / Integrity using Encryption | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-17(2) | AC-17(2) Remote Access \| Protection of Confidentiality / Integrity using Encryption | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(2) | AC-17(2) Remote Access \| Protection of Confidentiality / Integrity using Encryption | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(2) | AC-17(2) Remote Access \| Protection of Confidentiality / Integrity using Encryption | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(2) | AC-17(2) Remote Access \| Protection of Confidentiality / Integrity using Encryption | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-AC-17(2) | AC-17(2) Remote Access \| Protection of Confidentiality / Integrity using Encryption | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(3) | AC-17(3) Remote Access \| Managed Access Control Points | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(4) | AC-17(4) Remote Access \| Privileged Commands / Access | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(4) | AC-17(4) Remote Access \| Privileged Commands / Access | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17(4) | AC-17(4) Remote Access \| Privileged Commands / Access | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-17.A | AC-17.A Remote Access | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-17.AA | AC-17.AA Remote Access | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AC-17.B | AC-17.B Remote Access | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.A | AU-2.A Audit Events | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.B | AU-2.B Audit Events | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.C | AU-2.C Audit Events | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-2.D | AU-2.D Audit Events | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3(1) | AU-3(1) Content of Audit Records \| Additional Audit Information | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-3.A | AU-3.A Content of Audit Records | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-5.A | AU-5.A Response to Audit Processing Failures | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-5.B | AU-5.B Response to Audit Processing Failures | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) Audit Review, Analysis, and Reporting \| Process Integration | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) Audit Review, Analysis, and Reporting \| Process Integration | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-AU-6(1) | AU-6(1) Audit Review, Analysis, and Reporting \| Process Integration | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) Audit Review, Analysis, and Reporting \| Process Integration | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) Audit Review, Analysis, and Reporting \| Process Integration | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(1) | AU-6(1) Audit Review, Analysis, and Reporting \| Process Integration | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-6(3) | AU-6(3) Audit Review, Analysis, and Reporting \| Correlate Audit Repositories | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-AU-7(1) | AU-7(1) Audit Reduction and Report Generation \| Automatic Processing | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-8.B | AU-8.B Time Stamps | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-9(2) | AU-9(2) Protection of Audit Information \| Audit Backup on Separate Physical Systems / Components | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-9(2) | AU-9(2) Protection of Audit Information \| Audit Backup on Separate Physical Systems / Components | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-AU-9(2) | AU-9(2) Protection of Audit Information \| Audit Backup on Separate Physical Systems / Components | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-9.A | AU-9.A Protection of Audit Information | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| CCCS-fPBMM-AU-9.A | AU-9.A Protection of Audit Information | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-9.A | AU-9.A Protection of Audit Information | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| CCCS-fPBMM-AU-11.A | AU-11.A Audit Record Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-11.B | AU-11.B Audit Record Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| CCCS-fPBMM-AU-11.C | AU-11.C Audit Record Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.A | AU-12.A Audit Generation | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-AU-12.C | AU-12.C Audit Generation | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-3(5) | CA-3(5) System Interconnections \| Restrictions on External Network Connections | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.A | CA-7.A Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.B | CA-7.B Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.C | CA-7.C Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.D | CA-7.D Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.E | CA-7.E Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.F | CA-7.F Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | api-gw-xray-enabled | AWS X-Ray collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportuni ties for optimizat ion. Ensure X-Ray is enables so you can see detailed informati on not only about the request and response, but also about calls that your application makes to downstream AWS resources, microserv ices, databases and HTTP web APIs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-7.G | CA-7.G Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CA-9.A | CA-9.A Internal System Connections | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A Baseline Configuration | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A Baseline Configuration | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A Baseline Configuration | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CCCS-fPBMM-CM-2.A | CM-2.A Baseline Configuration | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A Baseline Configuration | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A Baseline Configuration | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-2.A | CM-2.A Baseline Configuration | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.A | CM-3.A Configuration Change Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.A | CM-3.A Configuration Change Control | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.B | CM-3.B Configuration Change Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.B | CM-3.B Configuration Change Control | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.C | CM-3.C Configuration Change Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.C | CM-3.C Configuration Change Control | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.D | CM-3.D Configuration Change Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.D | CM-3.D Configuration Change Control | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.E | CM-3.E Configuration Change Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.E | CM-3.E Configuration Change Control | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.F | CM-3F Configuration Change Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.F | CM-3F Configuration Change Control | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.G | CM-3.G Configuration Change Control | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-3.G | CM-3.G Configuration Change Control | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(1) | CM-5(1) Access Restrictions for Change \| Automated Access Enforcement / Auditing | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5(5) | CM-5(5) Access Restrictions for Change \| Limit Production / Operational Privileges | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-5.A | CM-5.A Access Restrictions for Change | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6(1) | CM-6(1) Configuration Settings \| Automated Central Management / Application / Verification | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6(1) | CM-6(1) Configuration Settings \| Automated Central Management / Application / Verification | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CM-6(1) | CM-6(1) Configuration Settings \| Automated Central Management / Application / Verification | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.A | CM-6.A Configuration Settings | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.B | CM-6.B Configuration Settings | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.C | CM-6.C Configuration Settings | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-6.D | CM-6.D Configuration Settings | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| CCCS-fPBMM-CM-7.A | CM-7.A Least Functionality | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-7.A | CM-7.A Least Functionality | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-7.B | CM-7.B Least Functionality | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-7.B | CM-7.B Least Functionality | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(1) | CM-8(1) Information System Component Inventory \| Updates During Installations / Removals | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(1) | CM-8(1) Information System Component Inventory \| Updates During Installations / Removals | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(2) | CM-8(2) Information System Component Inventory \| Automated Maintenance | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(2) | CM-8(2) Information System Component Inventory \| Automated Maintenance | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(3) | CM-8(3) Information System Component Inventory \| Automated Unauthorized Component Detection | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(3) | CM-8(3) Information System Component Inventory \| Automated Unauthorized Component Detection | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8(3) | CM-8(3) Information System Component Inventory \| Automated Unauthorized Component Detection | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-CM-8(3) | CM-8(3) Information System Component Inventory \| Automated Unauthorized Component Detection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.A | CM-8.A Information System Component Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.A | CM-8.A Information System Component Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.B | CM-8.B Information System Component Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.B | CM-8.B Information System Component Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.C | CM-8.C Information System Component Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.C | CM-8.C Information System Component Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.D | CM-8.D Information System Component Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.D | CM-8.D Information System Component Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.E | CM-8.E Information System Component Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CM-8.E | CM-8.E Information System Component Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(5) | CP-2(5) Contingency Plan \| Continue Essential Missions / Business Functions | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) Contingency Plan \| Alternate Processing / Storage Site | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) Contingency Plan \| Alternate Processing / Storage Site | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) Contingency Plan \| Alternate Processing / Storage Site | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) Contingency Plan \| Alternate Processing / Storage Site | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) Contingency Plan \| Alternate Processing / Storage Site | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2(6) | CP-2(6) Contingency Plan \| Alternate Processing / Storage Site | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.A | CP-2.A Contingency Plan | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.B | CP-2.B Contingency Plan | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.C | CP-2.C Contingency Plan | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.D | CP-2.D Contingency Plan | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.E | CP-2.E Contingency Plan | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.F | CP-2.F Contingency Plan | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-2.G | CP-2.G Contingency Plan | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-6(1) | CP-6(1) Alternate Storage Site \| Separation from Primary Site | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-6(2) | CP-6(2) Alternate Storage Site \| Recovery Times / Point Objectives | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-6.A | CP-6.A Alternate Storage Site | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-6.B | CP-6.B Alternate Storage Site | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | backup-recovery-po int-minimum-retent ion-check | To help with data back-up processes , ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. This rule allows you to set the requiredRetentionD ays (config default: 35) parameter. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | ebs-optimized-inst ance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/ O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contentio n between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | ebs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | ec2-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | efs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | rds-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-9(3) | CP-9(3) Informati on System Backup \| Separate Storage for Critical Information | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9(7) | CP-9(7) Information System Backup \| Dual Authorization | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |
| CCCS-fPBMM-CP-9(7) | CP-9(7) Information System Backup \| Dual Authorization | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-9.A | CP-9.A Information System Backup | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-9.AA | CP-9.AA Information System Backup | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | dynamodb-pitr-enabled | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-9.B | CP-9.B Information System Backup | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-9.C | CP-9.C Information System Backup | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | dynamodb-pitr-enabled | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-9.D | CP-9.D Information System Backup | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-CP-10.A | CP-10.A Information System Recovery and Reconstitution | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(1) | IA-2(1) Identification and Authentication (Organizational Users) \| Network Access to Privileged Accounts | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(1) | IA-2(1) Identification and Authentication (Organizational Users) \| Network Access to Privileged Accounts | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(1) | IA-2(1) Identification and Authentication (Organizational Users) \| Network Access to Privileged Accounts | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CCCS-fPBMM-IA-2(3) | IA-2(3) Identification and Authentication (Organizational Users) \| Local Access to Privileged Accounts | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(3) | IA-2(3) Identification and Authentication (Organizational Users) \| Local Access to Privileged Accounts | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(3) | IA-2(3) Identification and Authentication (Organizational Users) \| Local Access to Privileged Accounts | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CCCS-fPBMM-IA-2(8) | IA-2(8) Identification and Authentication (Organizational Users) \| Network Access to Privileged Accounts - Replay Resistant | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-IA-2(8) | IA-2(8) Identification and Authentication (Organizational Users) \| Network Access to Privileged Accounts - Replay Resistant | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(8) | IA-2(8) Identification and Authentication (Organizational Users) \| Network Access to Privileged Accounts - Replay Resistant | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CCCS-fPBMM-IA-2(11) | IA-2(11) Identification and Authentication (Organizational Users) \| Remote Access - Separate Device | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(11) | IA-2(11) Identification and Authentication (Organizational Users) \| Remote Access - Separate Device | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2(11) | IA-2(11) Identification and Authentication (Organizational Users) \| Remote Access - Separate Device | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2.A | IA-2.A Identification and Authentication (Organizational Users) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| CCCS-fPBMM-IA-2.A | IA-2.A Identification and Authentication (Organizational Users) | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2.A | IA-2.A Identification and Authentication (Organizational Users) | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-2.A | IA-2.A Identification and Authentication (Organizational Users) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4(4) | IA-4(4) Identifier Management \| Identify User Status | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.A | IA-4.A Identifier Management | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.A | IA-4.A Identifier Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.A | IA-4.A Identifier Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.B | IA-4.B Identifier Management | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.B | IA-4.B Identifier Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.B | IA-4.B Identifier Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.C | IA-4.C Identifier Management | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.C | IA-4.C Identifier Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.C | IA-4.C Identifier Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.D | IA-4.D Identifier Management | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.D | IA-4.D Identifier Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.D | IA-4.D Identifier Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.E | IA-4.E Identifier Management | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.E | IA-4.E Identifier Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-4.E | IA-4.E Identifier Management | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(1) | IA-5(1) Authenticator Management \| Password-Based Authentication | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| CCCS-fPBMM-IA-5(2) | IA-5(2) Authenticator Management \| PKI-Based Authentication | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(2) | IA-5(2) Authenticator Management \| PKI-Based Authentication | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(4) | IA-5(4) Authenticator Management \| Automated Support for Password Strength Determination | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(8) | IA-5(8) Authenticator Management \| Multiple Information System Accounts | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(8) | IA-5(8) Authenticator Management \| Multiple Information System Accounts | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5(8) | IA-5(8) Authenticator Management \| Multiple Information System Accounts | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.A | IA-5.A Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.A | IA-5.A Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.A | IA-5.A Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.A | IA-5.A Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.B | IA-5.B Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.B | IA-5.B Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.B | IA-5.B Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.B | IA-5.B Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.C | IA-5.C Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.C | IA-5.C Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.C | IA-5.C Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.C | IA-5.C Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.D | IA-5.D Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.D | IA-5.D Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.D | IA-5.D Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.D | IA-5.D Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.E | IA-5.E Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.E | IA-5.E Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.E | IA-5.E Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.E | IA-5.E Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.F | IA-5.F Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| CCCS-fPBMM-IA-5.F | IA-5.F Authenticator Management | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.F | IA-5.F Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.F | IA-5.F Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.G | IA-5.G Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.G | IA-5.G Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.G | IA-5.G Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.G | IA-5.G Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.H | IA-5.H Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.H | IA-5.H Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.H | IA-5.H Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.H | IA-5.H Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.I | IA-5.I Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.I | IA-5.I Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-IA-5.I | IA-5.I Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.I | IA-5.I Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.J | IA-5.J Authenticator Management | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| CCCS-fPBMM-IA-5.J | IA-5.J Authenticator Management | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.J | IA-5.J Authenticator Management | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-IA-5.J | IA-5.J Authenticator Management | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CCCS-fPBMM-IR-6(1) | IR-6(1) Incident Reporting \| Automated Reporting | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-3.A | MA-3.A Maintenance Tools | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-3.A | MA-3.A Maintenance Tools | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MA-4(1) | MA-4(1) Nonlocal Maintenance \| Auditing and Review | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-MP-2.A | MP-2.A Media Access | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| CCCS-fPBMM-RA-5.A | RA-5.A Vulnerability Scanning | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-RA-5.B | RA-5.B Vulnerability Scanning | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-RA-5.C | RA-5.C Vulnerability Scanning | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-RA-5.D | RA-5.D Vulnerability Scanning | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-RA-5.E | RA-5.E Vulnerability Scanning | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SA-10(1) | SA-10(1) Developer Configuration Management \| Software / Firmware Integrity Verification | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-5.A | SC-5.A Denial of Service Protection | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| CCCS-fPBMM-SC-5.A | SC-5.A Denial of Service Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-6.A | SC-6.A Resource Availability | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(3) | SC-7(3) Boundary Protection \| Access Points | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-7(4) | SC-7(4) Boundary Protection \| External Telecommunications Services | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(5) | SC-7(5) Boundary Protection \| Deny by Default / Allow by Exception | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(5) | SC-7(5) Boundary Protection \| Deny by Default / Allow by Exception | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(5) | SC-7(5) Boundary Protection \| Deny by Default / Allow by Exception | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(5) | SC-7(5) Boundary Protection \| Deny by Default / Allow by Exception | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-7(7) | SC-7(7) Boundary Protection \| Prevent Split Tunneling for Remote Devices | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.A | SC-7.A Boundary Protection | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.B | SC-7.B Boundary Protection | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-7.C | SC-7.C Boundary Protection | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8(1) | SC-8(1) Transmission Confidentiality and Integrity \| Cryptographic or Alternate Physical Protection | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-8.A | SC-8.A Transmission Confidentiality and Integrity | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-12(1) | SC-12(1) Cryptographic Key Establishment and Management \| Availability | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| CCCS-fPBMM-SC-12(2) | SC-12(2) Cryptographic Key Establishment and Management \| Symmetric Keys | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SC-12(2) | SC-12(2) Cryptographic Key Establishment and Management \| Symmetric Keys | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| CCCS-fPBMM-SC-12.A | SC-12.A Cryptographic Key Establishment and Management | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-12.A | SC-12.A Cryptographic Key Establishment and Management | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-13.A | SC-13.A Cryptographic Protection | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-22.A | SC-22.A Architecture and Provisioning for Name / Address Resolution Service | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-23.A | SC-23.A Session Authenticity | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28(1) | SC-28(1) Protection of Information at Rest \| Cryptographic Protection | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| CCCS-fPBMM-SC-28.A | SC-28.A Protection of Information at Rest | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(2) | SI-2(2) Flaw Remediation \| Automated Flaw Remediation Status | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2(3) | SI-2(3) Flaw Remediation \| Time to Remediate Flaws / Benchmarks for Corrective Actions | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.A | SI-2.A Flaw Remediation | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.B | SI-2.B Flaw Remediation | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.C | SI-2.C Flaw Remediation | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-2.D | SI-2.D Flaw Remediation | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3(1) | SI-3(1) Malicious Code Protection \| Central Management | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-3(7) | SI-3(7) Malicious Code Protection \| Non Signature-Based Detection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.A | SI-3.A Malicious Code Protection | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.A | SI-3.A Malicious Code Protection | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.A | SI-3.A Malicious Code Protection | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.A | SI-3.A Malicious Code Protection | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-3.A | SI-3.A Malicious Code Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.B | SI-3.B Malicious Code Protection | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.B | SI-3.B Malicious Code Protection | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.B | SI-3.B Malicious Code Protection | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-3.B | SI-3.B Malicious Code Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.C | SI-3.C Malicious Code Protection | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.C | SI-3.C Malicious Code Protection | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.C | SI-3.C Malicious Code Protection | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-3.C | SI-3.C Malicious Code Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.D | SI-3.D Malicious Code Protection | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.D | SI-3.D Malicious Code Protection | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-3.D | SI-3.D Malicious Code Protection | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CCCS-fPBMM-SI-3.D | SI-3.D Malicious Code Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(1) | SI-4(1) Information System Monitoring \| System-Wide Intrusion Detection System | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(1) | SI-4(1) Information System Monitoring \| System-Wide Intrusion Detection System | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(2) | SI-4(2) Information System Monitoring \| Automated Tools for Real-Time Analysis | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(2) | SI-4(2) Information System Monitoring \| Automated Tools for Real-Time Analysis | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(4) | SI-4(4) Information System Monitoring \| Inbound and Outbound Communications Traffic | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4(4) | SI-4(4) Information System Monitoring \| Inbound and Outbound Communications Traffic | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(5) | SI-4(5) Information System Monitoring \| System-Generated Alerts | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(11) | SI-4(11) Information System Monitoring \| Analyze Communications Traffic Anomalies | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(11) | SI-4(11) Information System Monitoring \| Analyze Communications Traffic Anomalies | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(16) | SI-4(16) Information System Monitoring \| Correlate Monitoring Information | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(16) | SI-4(16) Information System Monitoring \| Correlate Monitoring Information | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(20) | SI-4(20) Information System Monitoring \| Privileged User | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(23) | SI-4(23) Information System Monitoring \| Host-Based Devices | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4(23) | SI-4(23) Information System Monitoring \| Host-Based Devices | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.A | SI-4.A Information System Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.A | SI-4.A Information System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.A | SI-4.A Information System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4.A | SI-4.A Information System Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.A | SI-4.A Information System Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.B | SI-4.B Information System Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.B | SI-4.B Information System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.B | SI-4.B Information System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4.B | SI-4.B Information System Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.B | SI-4.B Information System Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.C | SI-4.C Information System Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.C | SI-4.C Information System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.C | SI-4.C Information System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4.C | SI-4.C Information System Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.C | SI-4.C Information System Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.D | SI-4.D Information System Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.D | SI-4.D Information System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.D | SI-4.D Information System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4.D | SI-4.D Information System Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.D | SI-4.D Information System Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.E | SI-4.E Information System Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.E | SI-4.E Information System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.E | SI-4.E Information System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4.E | SI-4.E Information System Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.E | SI-4.E Information System Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.F | SI-4.F Information System Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.F | SI-4.F Information System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.F | SI-4.F Information System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4.F | SI-4.F Information System Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.F | SI-4.F Information System Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.G | SI-4.G Information System Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.G | SI-4.G Information System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.G | SI-4.G Information System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-4.G | SI-4.G Information System Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-4.G | SI-4.G Information System Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-5.A | SI-5.A Security Alerts, Advisories, and Directives | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-5.B | SI-5.B Security Alerts, Advisories, and Directives | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-5.C | SI-5.C Security Alerts, Advisories, and Directives | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CCCS-fPBMM-SI-5.D | SI-5.D Security Alerts, Advisories, and Directives | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-7(1) | SI-7(1) Software, Firmware, and Information Integrity \| Integrity Checks | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-7(7) | SI-7(7) Software, Firmware, and Information Integrity \| Integration of Detection and Response | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-7.A | SI-7.A Software, Firmware, and Information Integrity | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CCCS-fPBMM-SI-12.A | SI-12.A Information Handling and Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

### Template

The template is available on GitHub: Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile.

## Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 1 and AWS managed Config rules/AWS Config Process Checks. Each Config rule applies to a specific AWS resource, and relates to one or more CIS Amazon Web Services Foundation v1.4 Level 1 controls. A CIS Amazon Web Services Foundation v1.4 Level 1 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

For more information about process checks, see process-checks.

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.1 | Maintain current contact details | account-contact-details-configured (process check) | Ensure the contact email and telephone number for AWS accounts are current and map to more than one individua l in your organizat ion. Within the My Account section of the console ensure correct information is specified in the Contact Informati on section. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_servic es/ |
| 1.2 | Ensure security contact information is registered | account-security-c ontact-configured (Process Check) | Ensure the contact email and telephone number for the your organizations security team are current. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | Within the My Account section of the AWS Management Console ensure the correct information is specified in the Security section. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4 | Ensure no 'root' user access key exists | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5 | Ensure MFA is enabled for the 'root' user | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.7 | Eliminate use of the 'root' user for administrative and daily tasks | root-account-regular-use (Process Check) | Ensure the use of the root account is avoided for everyday tasks. Within IAM, run a credential report to examine when the root user was last used. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.8 | Ensure IAM password policy requires minimum length of 14 or greater | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.9 | Ensure IAM password policy prevents password reuse | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.10 | Ensure multi-factor authentication (MFA) is enabled for all users that have a console password | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.11 | Do not setup access keys during initial user setup for all users that have a console password | iam-user-console-and-api-access-at-creation (Process Check) | Ensure access keys are not setup during the initial user setup for all users that have a console password. For all users with console access, compare the user 'Creation time` to the Access Key `Created` date. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.12 | Ensure credentials unused for 45 days or greater are disabled | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (CIS Standard value: 45). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.13 | Ensure there is only one active access key available for any single user | iam-user-single-access-key (Process Check) | Ensure there is only one active access key available for any single user. For all users check that there is only one active key used within the Security Credentials tab for each user within IAM. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.14 | Ensure access keys are rotated every 90 days or less | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.15 | Ensure users Receive Permissions Only Through Groups | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 1.15 | Ensure users Receive Permissions Only Through Groups | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.15 | Ensure users Receive Permissions Only Through Groups | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.16 | Ensure IAM policies that allow full "*:*" administrative privileges are not attached | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.17 | Ensure a support role has been created to manage incidents with AWS Support | iam-policy-in-use | AWS Identity and Access Management (IAM) can help you manage access permissions and authorizations by ensuring that IAM policies are assigned to the appropriate users, roles, or groups. Restricting these policies also incorporates the principals of least privilege and separation of duties. This rule requires that you set the policyARN to arn:aws:iam::aws:policy/AWSSupportAccess, for incident management with AWS Support. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.19 | Ensure that all the expired SSL/TLS certificates stored in AWS IAM are removed | iam-expired-certificates (Process Check) | Ensure that all the expired SSL/TLS certificates stored in IAM are removed. From the command line with the installed AWS CLI run the 'AWS iam list-server-certificates' command and determine if there are any expired server certificates. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.20 | Ensure that AWS IAM Access Analyzer is enabled | iam-access-analyzer-enabled (Process Check) | Ensure that IAM Access Analyzer is enabled. Within the IAM section of the console, select Access Analyzer and ensure that the STATUS is set to Active. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1.3 | Ensure MFA Delete is enable on S3 buckets | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Adding multi factor authentication (MFA) delete to an S3 bucket requires an additional factor of authentication in order to change the version state of your bucket or to delete and object version. MFA delete can add an additional layer of security in the event security credentials are compromised or unauthorized access is granted. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1.5 | Ensure that S3 Buckets are configure d with 'Block public access (bucket settings)' | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1.5 | Ensure that S3 Buckets are configured with 'Block public access (bucket settings)' | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 2.2.1 | Ensure EBS volume encryption is enabled | encrypted-volumes | Because senstive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.1 | Ensure EBS volume encryption is enabled | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 2.3.1 | Ensure that encryption is enabled for RDS Instances | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.3.1 | Ensure that encryption is enabled for RDS Instances | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1 | Ensure CloudTrail is enabled in all regions | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.3 | Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.4 | Ensure CloudTrail trails are integrated with CloudWatch Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6 | Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Ensure a log metric filter and alarm exist for unauthorized API calls | alarm-unauthorized-api-calls (Process Check) | Ensure a log metric filter and an alarm exists for unauthorized API calls. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2 | Ensure a log metric filter and alarm exist for Managemen t Console sign-in without MFA | alarm-sign-in-with out-mfa (Process Check) | Ensure a log metric filter and an alarm exists for AWS Management Console sign-in without Multi-Factor Authentic ation (MFA). For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_servic es/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3 | Ensure a log metric filter and alarm exist for usage of 'root' account | alarm-root-account-use (Process Check) | Ensure a log metric filter and an alarm exists for usage of the root account. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4 | Ensure a log metric filter and alarm exist for IAM policy changes | alarm-iam-policy-change (Process Check) | Ensure a log metric filter and an alarm exists for IAM policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.5 | Ensure a log metric filter and alarm exist for CloudTrail configuration changes | alarm-cloudtrail-config-change (Process Check) | Ensure a log metric filter and an alarm exists for AWS CloudTrail configuration changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8 | Ensure a log metric filter and alarm exist for S3 bucket policy changes | alarm-s3-bucket-policy-change (Process Check) | Ensure a log metric filter and an alarm exists for Amazon S3 bucket policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.12 | Ensure a log metric filter and alarm exist for changes to network gateways | alarm-vpc-network-gateway-change (Process Check) | Ensure a log metric filter and an alarm exists for changes to network gateways. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.13 | Ensure a log metric filter and alarm exist for route table changes | alarm-vpc-route-table-change (Process Check) | Ensure a log metric filter and an alarm exists for route table changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.14 | Ensure a log metric filter and alarm exist for VPC changes | alarm-vpc-change (Process Check) | Ensure a log metric filter and an alarm exists for Amazon Virtual Private Cloud (VPC) changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.15 | Ensure a log metric filter and alarm exists for AWS Organizat ions changes | alarm-organization s-change (Process Check) | Ensure a log metric filter and an alarm exists for AWS Organizat ions changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.1 | Ensure no Network ACLs allow ingress from 0.0.0.0/0 to remote server administration ports | nacl-no-unrestricted-ssh-rdp | Ensure no network ACLs allow public ingress to the remote server administr ation ports. Within the VPC section of the console, ensure there are network ACLs with a source of '0.0.0.0/0' with allowing ports or port ranges including remote server admin ports. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (CIS Standard value: 3389). The actual values should reflect your organization's policies. |

## Template

The template is available on GitHub: Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1.

# Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 2 and AWS managed Config rules/AWS Config Process Checks. Each Config rule applies to a specific AWS resource, and relates to one or more CIS Amazon Web Services Foundation v1.4 Level 2 controls. A CIS Amazon Web Services Foundation v1.4 Level 2 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

For more information about process checks, see process-checks.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.1 | Maintain current contact details | account-contact-details-configured (process check) | Ensure the contact email and telephone number for AWS accounts are current and map to more than one individua l in your organizat ion. Within the My Account section of the console ensure correct information is specified in the Contact Informati on section. For further details on the auditing |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2 | Ensure security contact information is registered | account-security-contact-configured (Process Check) | Ensure the contact email and telephone number for the your organizations security team are current. Within the My Account section of the AWS Management Console ensure the correct information is specified in the Security section. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4 | Ensure no 'root' user access key exists | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5 | Ensure MFA is enabled for the 'root' user | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.6 | Ensure hardware MFA is enabled for the 'root' user account | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.7 | Eliminate use of the 'root' user for administrative and daily tasks | root-account-regular-use (Process Check) | Ensure the use of the root account is avoided for everyday tasks. Within IAM, run a credential report to examine when the root user was last used. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.8 | Ensure IAM password policy requires minimum length of 14 or greater | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.9 | Ensure IAM password policy prevents password reuse | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.10 | Ensure multi-factor authentication (MFA) is enabled for all users that have a console password | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.11 | Do not setup access keys during initial user setup for all users that have a console password | iam-user-console-and-api-access-at-creation (Process Check) | Ensure access keys are not setup during the initial user setup for all users that have a console password. For all users with console access, compare the user 'Creation time` to the Access Key `Created` date. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.12 | Ensure credentials unused for 45 days or greater are disabled | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (CIS Standard value: 45). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.13 | Ensure there is only one active access key available for any single user | iam-user-single-access-key (Process Check) | Ensure there is only one active access key available for any single user. For all users check that there is only one active key used within the Security Credentials tab for each user within IAM. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.14 | Ensure access keys are rotated every 90 days or less | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.15 | Ensure users Receive Permissions Only Through Groups | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 1.15 | Ensure users Receive Permissions Only Through Groups | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.15 | Ensure users Receive Permissions Only Through Groups | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.16 | Ensure IAM policies that allow full "*:*" administrative privileges are not attached | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.17 | Ensure a support role has been created to manage incidents with AWS Support | iam-policy-in-use | AWS Identity and Access Managemen t (IAM) can help you manage access permissions and authorizations by ensuring that IAM policies are assigned to the appropria te users, roles, or groups. Restricti ng these policies also incorporates the principals of least privilege and separation of duties. This rule requires that you set the policyARN to arn:aws:iam::aws:p olicy/AWSSupportAc cess, for incident management with AWS Support. |
| 1.18 | Ensure IAM instance roles are used for AWS resource access from instances | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.19 | Ensure that all the expired SSL/TLS certificates stored in AWS IAM are removed | iam-expired-certificates (Process Check) | Ensure that all the expired SSL/TLS certificates stored in IAM are removed. From the command line with the installed AWS CLI run the 'AWS iam list-server-certificates' command and determine if there are any expired server certificates. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.20 | Ensure that AWS IAM Access Analyzer is enabled | iam-access-analyzer-enabled (Process Check) | Ensure that IAM Access Analyzer is enabled. Within the IAM section of the console, select Access Analyzer and ensure that the STATUS is set to Active. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.21 | Ensure users are managed centrally from the identity federation or AWS Organizations for multi-account environments | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 2.1.1 | Ensure all S3 buckets employ encryption-at-rest | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.1.2 | Ensure S3 Bucket Policy is set to deny HTTP requests | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1.3 | Ensure MFA Delete is enable on S3 buckets | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Adding multi factor authentication (MFA) delete to an S3 bucket requires an additional factor of authentication in order to change the version state of your bucket or to delete and object version. MFA delete can add an additional layer of security in the event security credentials are compromised or unauthorized access is granted. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.1.5 | Ensure that S3 Buckets are configure d with 'Block public access (bucket settings)' | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.1.5 | Ensure that S3 Buckets are configured with 'Block public access (bucket settings)' | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 2.2.1 | Ensure EBS volume encryption is enabled | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2.1 | Ensure EBS volume encryption is enabled | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 2.3.1 | Ensure that encryption is enabled for RDS Instances | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.3.1 | Ensure that encryption is enabled for RDS Instances | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1 | Ensure CloudTrail is enabled in all regions | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2 | Ensure CloudTrail log file validation is enabled | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.3 | Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.4 | Ensure CloudTrail trails are integrated with CloudWatch Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5 | Ensure AWS Config is enabled in all regions | config-enabled-all-regions (Process Check) | Ensure AWS Config is enabled in all AWS Regions. Within the AWS Config section of the console, for each Region enabled ensure the AWS Config recorder is configured correctly. Ensure recording of global AWS resources is enabled at least in one Region. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6 | Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 3.7 | Ensure CloudTrail logs are encrypted at rest using KMS CMKs | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.8 | Ensure rotation for customer created CMKs is enabled | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |
| 3.9 | Ensure VPC flow logging is enabled in all VPCs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Ensure that Object-level logging for write events is enabled for S3 bucket | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 3.11 | Ensure that Object-level logging for read events is enabled for S3 bucket | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Ensure a log metric filter and alarm exist for unauthorized API calls | alarm-unauthorized-api-calls (Process Check) | Ensure a log metric filter and an alarm exists for unauthorized API calls. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2 | Ensure a log metric filter and alarm exist for Managemen t Console sign-in without MFA | alarm-sign-in-with out-mfa (Process Check) | Ensure a log metric filter and an alarm exists for AWS Management Console sign-in without Multi-Factor Authentic ation (MFA). For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_servic es/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3 | Ensure a log metric filter and alarm exist for usage of 'root' account | alarm-root-account-use (Process Check) | Ensure a log metric filter and an alarm exists for usage of the root account. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4 | Ensure a log metric filter and alarm exist for IAM policy changes | alarm-iam-policy-change (Process Check) | Ensure a log metric filter and an alarm exists for IAM policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.5 | Ensure a log metric filter and alarm exist for CloudTrail configuration changes | alarm-cloudtrail-config-change (Process Check) | Ensure a log metric filter and an alarm exists for AWS CloudTrail configuration changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.6 | Ensure a log metric filter and alarm exist for AWS Management Console authentication failures | alarm-console-auth-failures (Process Check) | Ensure a log metric filter and an alarm exists for AWS Management Console authentication failures. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.7 | Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs | alarm-kms-disable-or-delete-cmk (Process Check) | Ensure a log metric filter and an alarm exists for disabling or scheduled deletion of customer created CMKs. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8 | Ensure a log metric filter and alarm exist for S3 bucket policy changes | alarm-s3-bucket-policy-change (Process Check) | Ensure a log metric filter and an alarm exists for Amazon S3 bucket policy changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.9 | Ensure a log metric filter and alarm exist for AWS Config configuration changes | alarm-aws-config-change (Process Check) | Ensure a log metric filter and an alarm exists for AWS Config configura tion changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.10 | Ensure a log metric filter and alarm exist for security group changes | alarm-vpc-secrity-group-change (Process Check) | Ensure a log metric filter and an alarm exists for security group changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.11 | Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL) | alarm-vpc-nacl-change (Process Check) | Ensure a log metric filter and an alarm exists for changes to Network Access Control Lists (NACL). For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.12 | Ensure a log metric filter and alarm exist for changes to network gateways | alarm-vpc-network-gateway-change (Process Check) | Ensure a log metric filter and an alarm exists for changes to network gateways. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.13 | Ensure a log metric filter and alarm exist for route table changes | alarm-vpc-route-table-change (Process Check) | Ensure a log metric filter and an alarm exists for route table changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.14 | Ensure a log metric filter and alarm exist for VPC changes | alarm-vpc-change (Process Check) | Ensure a log metric filter and an alarm exists for Amazon Virtual Private Cloud (VPC) changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.15 | Ensure a log metric filter and alarm exists for AWS Organizat ions changes | alarm-organization s-change (Process Check) | Ensure a log metric filter and an alarm exists for AWS Organizat ions changes. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.1 | Ensure no Network ACLs allow ingress from 0.0.0.0/0 to remote server administration ports | nacl-no-unrestricted-ssh-rdp | Ensure no network ACLs allow public ingress to the remote server administr ation ports. Within the VPC section of the console, ensure there are network ACLs with a source of '0.0.0.0/0' with allowing ports or port ranges including remote server admin ports. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.2 | Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.2 | Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration ports | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (CIS Standard value: 3389). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3 | Ensure the default security group of every VPC restricts all traffic | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4 | Ensure routing tables for VPC peering are "least access" | vpc-peering-least-access (Process Check) | Ensure the routing tables for Amazon VPC peering are "least access". Within the VPC section of the console, examine the route table entries to ensure that the least number of subnets or hosts are required to accomplish the purpose for peering are routable. For further details on the auditing of this control please refer to the CIS Amazon Web Services Foundations Benchmark version 1.4.0 document available at https://www.cisecurity.org/benchmark/amazon_web_services/ |

## Template

The template is available on GitHub: Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2.

# Operational Best Practices for CIS Critical Security Controls v8 IG1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Critical Security Controls v8 IG1 and AWS managed Config rules. Each AWS Config applies to a specific AWS resource, and relates to one or more CIS Critical Security Controls v8 IG1 controls. A CIS Critical Security Controls v8 IG1 control can be related to multiple AWS Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-security-group-attached-to-eni | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2 | Ensure Authorized Software is Currently Supported | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 2.2 | Ensure Authorized Software is Currently Supported | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Ensure Authorized Software is Currently Supported | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| 3.3 | Configure Data Access Control Lists | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.3 | Configure Data Access Control Lists | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| 3.3 | Configure Data Access Control Lists | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 3.3 | Configure Data Access Control Lists | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 3.3 | Configure Data Access Control Lists | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.3 | Configure Data Access Control Lists | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.3 | Configure Data Access Control Lists | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 3.3 | Configure Data Access Control Lists | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| 3.3 | Configure Data Access Control Lists | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| 3.3 | Configure Data Access Control Lists | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Enforce Data Retention | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| 3.4 | Enforce Data Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Establish and Maintain a Secure Configuration Process | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 4.1 | Establish and Maintain a Secure Configuration Process | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.6 | Securely Manage Enterprise Assets and Software | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.6 | Securely Manage Enterprise Assets and Software | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.7 | Manage Default Accounts on Enterprise Assets and Software | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 5.1 | Establish and Maintain an Inventory of Accounts | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 5.2 | Use Unique Passwords | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3 | Disable Dormant Accounts | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4 | Require MFA for Remote Network Access | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4 | Require MFA for Remote Network Access | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4 | Require MFA for Remote Network Access | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.5 | Require MFA for Administrative Access | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 7.1 | Establish and Maintain a Vulnerability Management Process | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1 | Establish and Maintain a Vulnerability Management Process | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1 | Establish and Maintain a Vulnerability Management Process | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 7.3 | Perform Automated Operating System Patch Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3 | Perform Automated Operating System Patch Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3 | Perform Automated Operating System Patch Management | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.4 | Perform Automated Application Patch Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 7.4 | Perform Automated Application Patch Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.4 | Perform Automated Application Patch Management | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | Establish and Maintain an Audit Log Management Process | audit-log-policy-exists (Process check) | Establish and maintain an audit log management policy that defines your organization's logging requirements. This includes, but is not limited to, review and retention of audit logs. |
| 8.2 | Collect Audit Logs | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2 | Collect Audit Logs | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 8.2 | Collect Audit Logs | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 8.2 | Collect Audit Logs | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 8.3 | Ensure Adequate Audit Log Storage | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.1 | Deploy and Maintain Anti-Malware Software | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 10.2 | Configure Automatic Anti-Malware Signature Updates | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 11.2 | Perform Automated Backups | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | Perform Automated Backups | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 11.2 | Perform Automated Backups | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.3 | Protect Recovery Data | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 11.3 | Protect Recovery Data | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 11.3 | Protect Recovery Data | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.3 | Protect Recovery Data | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

## Template

The template is available on GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG1.

# Operational Best Practices for CIS Critical Security Controls v8 IG2

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Critical Security Controls v8 IG2 and AWS managed Config rules. Each AWS Config applies to a specific AWS resource, and relates to one or more CIS Critical Security Controls v8 IG2 controls. A CIS Critical Security Controls v8 IG2 control can be related to multiple AWS Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | eip-attached | This rule ensures Elastic IPs allocated to an Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-security-group-attached-to-eni | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2 | Ensure Authorized Software is Currently Supported | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 2.2 | Ensure Authorized Software is Currently Supported | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Ensure Authorized Software is Currently Supported | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.4 | Utilize Automated Software Inventory Tools | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.4 | Utilize Automated Software Inventory Tools | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| 3.3 | Configure Data Access Control Lists | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.3 | Configure Data Access Control Lists | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| 3.3 | Configure Data Access Control Lists | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 3.3 | Configure Data Access Control Lists | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 3.3 | Configure Data Access Control Lists | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.3 | Configure Data Access Control Lists | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.3 | Configure Data Access Control Lists | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 3.3 | Configure Data Access Control Lists | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| 3.3 | Configure Data Access Control Lists | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| 3.3 | Configure Data Access Control Lists | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Enforce Data Retention | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| 3.4 | Enforce Data Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.10 | Encrypt Sensitive Data in Transit | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| 3.10 | Encrypt Sensitive Data in Transit | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.10 | Encrypt Sensitive Data in Transit | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.10 | Encrypt Sensitive Data in Transit | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.10 | Encrypt Sensitive Data in Transit | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 3.11 | Encrypt Sensitive Data at Rest | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.11 | Encrypt Sensitive Data at Rest | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 3.11 | Encrypt Sensitive Data at Rest | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.11 | Encrypt Sensitive Data at Rest | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 3.11 | Encrypt Sensitive Data at Rest | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.11 | Encrypt Sensitive Data at Rest | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 4.1 | Establish and Maintain a Secure Configuration Process | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 4.1 | Establish and Maintain a Secure Configuration Process | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.6 | Securely Manage Enterprise Assets and Software | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.6 | Securely Manage Enterprise Assets and Software | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.7 | Manage Default Accounts on Enterprise Assets and Software | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 5.1 | Establish and Maintain an Inventory of Accounts | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 5.2 | Use Unique Passwords | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3 | Disable Dormant Accounts | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.6 | Centralize Account Management | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 6.4 | Require MFA for Remote Network Access | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4 | Require MFA for Remote Network Access | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4 | Require MFA for Remote Network Access | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.5 | Require MFA for Administrative Access | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 6.7 | Centralize Access Control | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1 | Establish and Maintain a Vulnerability Management Process | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1 | Establish and Maintain a Vulnerability Management Process | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1 | Establish and Maintain a Vulnerability Management Process | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 7.3 | Perform Automated Operating System Patch Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3 | Perform Automated Operating System Patch Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3 | Perform Automated Operating System Patch Management | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.4 | Perform Automated Application Patch Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 7.4 | Perform Automated Application Patch Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.4 | Perform Automated Application Patch Management | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.5 | Perform Automated Vulnerability Scans of Internal Enterprise Assets | ecr-private-image-scanning-enabled | Amazon Elastic Container Repositor y (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |
| 8.1 | Establish and Maintain an Audit Log Management Process | audit-log-policy-e xists (Process check) | Establish and maintain an audit log management policy that defines your organization's logging requireme nts. This includes, but is not limited to, review and retention of audit logs. |
| 8.2 | Collect Audit Logs | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 8.2 | Collect Audit Logs | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 8.2 | Collect Audit Logs | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 8.3 | Ensure Adequate Audit Log Storage | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 8.5 | Collect Detailed Audit Logs | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 8.5 | Collect Detailed Audit Logs | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 8.5 | Collect Detailed Audit Logs | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.7 | Collect URL Request Audit Logs | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| 8.9 | Centralize Audit Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.10 | Retain Audit Logs | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| 8.10 | Retain Audit Logs | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.1 | Deploy and Maintain Anti-Malware Software | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 10.2 | Configure Automatic Anti-Malware Signature Updates | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.4 | Configure Automatic Anti-Malware Scanning of Removable Media | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 10.6 | Centrally Manage Anti-Malware Software | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.7 | Use Behavior-Based Anti-Malware Software | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 11.2 | Perform Automated Backups | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | Perform Automated Backups | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 11.2 | Perform Automated Backups | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | Perform Automated Backups | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 11.2 | Perform Automated Backups | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.3 | Protect Recovery Data | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 11.3 | Protect Recovery Data | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 11.3 | Protect Recovery Data | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.3 | Protect Recovery Data | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 12.2 | Establish and Maintain a Secure Network Architecture | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 12.2 | Establish and Maintain a Secure Network Architecture | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| 12.2 | Establish and Maintain a Secure Network Architecture | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 12.2 | Establish and Maintain a Secure Network Architecture | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 12.2 | Establish and Maintain a Secure Network Architecture | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 12.2 | Establish and Maintain a Secure Network Architecture | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 12.2 | Establish and Maintain a Secure Network Architecture | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 12.2 | Establish and Maintain a Secure Network Architecture | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 12.2 | Establish and Maintain a Secure Network Architecture | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |
| 12.3 | Securely Manage Network Infrastructure | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.3 | Securely Manage Network Infrastructure | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.3 | Securely Manage Network Infrastructure | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.3 | Securely Manage Network Infrastructure | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.3 | Securely Manage Network Infrastructure | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.3 | Securely Manage Network Infrastructure | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.3 | Securely Manage Network Infrastructure | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 12.3 | Securely Manage Network Infrastructure | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.6 | Use of Secure Network Management and Communication Protocols | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 12.6 | Use of Secure Network Management and Communication Protocols | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.6 | Use of Secure Network Management and Communication Protocols | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 12.6 | Use of Secure Network Management and Communication Protocols | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.6 | Use of Secure Network Management and Communication Protocols | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.6 | Use of Secure Network Management and Communication Protocols | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.6 | Use of Secure Network Management and Communication Protocols | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 12.6 | Use of Secure Network Management and Communication Protocols | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13.1 | Centralize Security Event Alerting | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13.1 | Centralize Security Event Alerting | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 13.3 | Deploy a Network Intrusion Detection Solution | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 13.6 | Collect Network Traffic Flow Logs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13.6 | Collect Network Traffic Flow Logs | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

### Template

The template is available on GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG2.

## Operational Best Practices for CIS Critical Security Controls v8 IG3

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Critical Security Controls v8 IG3 and AWS managed Config rules. Each AWS Config applies to a specific AWS resource, and relates to one or more CIS Critical Security Controls v8 IG3 controls. A CIS Critical Security Controls v8 IG3 control can be related to multiple AWS Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | vpc-network-acl-un used-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | ec2-security-group-attached-to-eni | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2 | Ensure Authorized Software is Currently Supported | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 2.2 | Ensure Authorized Software is Currently Supported | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Ensure Authorized Software is Currently Supported | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.4 | Utilize Automated Software Inventory Tools | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.4 | Utilize Automated Software Inventory Tools | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| 3.3 | Configure Data Access Control Lists | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.3 | Configure Data Access Control Lists | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| 3.3 | Configure Data Access Control Lists | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 3.3 | Configure Data Access Control Lists | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 3.3 | Configure Data Access Control Lists | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3 | Configure Data Access Control Lists | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 3.3 | Configure Data Access Control Lists | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.3 | Configure Data Access Control Lists | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.3 | Configure Data Access Control Lists | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 3.3 | Configure Data Access Control Lists | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| 3.3 | Configure Data Access Control Lists | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Configure Data Access Control Lists | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| 3.3 | Configure Data Access Control Lists | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Enforce Data Retention | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| 3.4 | Enforce Data Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| 3.10 | Encrypt Sensitive Data in Transit | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.10 | Encrypt Sensitive Data in Transit | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.10 | Encrypt Sensitive Data in Transit | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.10 | Encrypt Sensitive Data in Transit | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.10 | Encrypt Sensitive Data in Transit | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 3.11 | Encrypt Sensitive Data at Rest | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 3.11 | Encrypt Sensitive Data at Rest | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 3.11 | Encrypt Sensitive Data at Rest | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| 3.11 | Encrypt Sensitive Data at Rest | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11 | Encrypt Sensitive Data at Rest | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 3.14 | Log Sensitive Data Access | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 3.14 | Log Sensitive Data Access | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 3.14 | Log Sensitive Data Access | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14 | Log Sensitive Data Access | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.14 | Log Sensitive Data Access | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Establish and Maintain a Secure Configuration Process | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Establish and Maintain a Secure Configuration Process | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 4.1 | Establish and Maintain a Secure Configuration Process | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Establish and Maintain a Secure Configuration Process | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.6 | Securely Manage Enterprise Assets and Software | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.6 | Securely Manage Enterprise Assets and Software | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4.6 | Securely Manage Enterprise Assets and Software | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.7 | Manage Default Accounts on Enterprise Assets and Software | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 5.1 | Establish and Maintain an Inventory of Accounts | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.2 | Use Unique Passwords | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 5.2 | Use Unique Passwords | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Use Unique Passwords | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3 | Disable Dormant Accounts | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.6 | Centralize Account Management | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 6.4 | Require MFA for Remote Network Access | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4 | Require MFA for Remote Network Access | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4 | Require MFA for Remote Network Access | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.5 | Require MFA for Administrative Access | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 6.7 | Centralize Access Control | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1 | Establish and Maintain a Vulnerability Management Process | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1 | Establish and Maintain a Vulnerability Management Process | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1 | Establish and Maintain a Vulnerability Management Process | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 7.3 | Perform Automated Operating System Patch Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3 | Perform Automated Operating System Patch Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3 | Perform Automated Operating System Patch Management | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.4 | Perform Automated Application Patch Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 7.4 | Perform Automated Application Patch Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.4 | Perform Automated Application Patch Management | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.5 | Perform Automated Vulnerability Scans of Internal Enterprise Assets | ecr-private-image-scanning-enabled | Amazon Elastic Container Repositor y (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |
| 8.1 | Establish and Maintain an Audit Log Management Process | audit-log-policy-e xists (Process check) | Establish and maintain an audit log management policy that defines your organization's logging requireme nts. This includes, but is not limited to, review and retention of audit logs. |
| 8.2 | Collect Audit Logs | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 8.2 | Collect Audit Logs | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2 | Collect Audit Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 8.2 | Collect Audit Logs | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2 | Collect Audit Logs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2 | Collect Audit Logs | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 8.3 | Ensure Adequate Audit Log Storage | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 8.5 | Collect Detailed Audit Logs | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 8.5 | Collect Detailed Audit Logs | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.5 | Collect Detailed Audit Logs | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| 8.5 | Collect Detailed Audit Logs | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.7 | Collect URL Request Audit Logs | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| 8.9 | Centralize Audit Logs | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.10 | Retain Audit Logs | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| 8.10 | Retain Audit Logs | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Deploy and Maintain Anti-Malware Software | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 10.2 | Configure Automatic Anti-Malware Signature Updates | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4 | Configure Automatic Anti-Malware Scanning of Removable Media | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 10.6 | Centrally Manage Anti-Malware Software | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.7 | Use Behavior-Based Anti-Malware Software | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 11.2 | Perform Automated Backups | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 11.2 | Perform Automated Backups | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | Perform Automated Backups | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | Perform Automated Backups | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | Perform Automated Backups | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 11.2 | Perform Automated Backups | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Protect Recovery Data | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 11.3 | Protect Recovery Data | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 11.3 | Protect Recovery Data | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.3 | Protect Recovery Data | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 11.4 | Establish and Maintain an Isolated Instance of Recovery Data | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 12.2 | Establish and Maintain a Secure Network Architecture | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 12.2 | Establish and Maintain a Secure Network Architecture | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| 12.2 | Establish and Maintain a Secure Network Architecture | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 12.2 | Establish and Maintain a Secure Network Architecture | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 12.2 | Establish and Maintain a Secure Network Architecture | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 12.2 | Establish and Maintain a Secure Network Architecture | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 12.2 | Establish and Maintain a Secure Network Architecture | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 12.2 | Establish and Maintain a Secure Network Architecture | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 12.2 | Establish and Maintain a Secure Network Architecture | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.2 | Establish and Maintain a Secure Network Architecture | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.2 | Establish and Maintain a Secure Network Architecture | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |
| 12.3 | Securely Manage Network Infrastructure | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.3 | Securely Manage Network Infrastructure | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.3 | Securely Manage Network Infrastructure | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.3 | Securely Manage Network Infrastructure | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.3 | Securely Manage Network Infrastructure | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.3 | Securely Manage Network Infrastructure | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.3 | Securely Manage Network Infrastructure | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 12.3 | Securely Manage Network Infrastructure | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.6 | Use of Secure Network Management and Communication Protocols | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 12.6 | Use of Secure Network Management and Communication Protocols | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.6 | Use of Secure Network Management and Communication Protocols | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 12.6 | Use of Secure Network Management and Communication Protocols | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.6 | Use of Secure Network Management and Communication Protocols | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 12.6 | Use of Secure Network Management and Communication Protocols | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.6 | Use of Secure Network Management and Communication Protocols | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 12.6 | Use of Secure Network Management and Communication Protocols | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13.1 | Centralize Security Event Alerting | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13.1 | Centralize Security Event Alerting | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 13.3 | Deploy a Network Intrusion Detection Solution | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 13.6 | Collect Network Traffic Flow Logs | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13.6 | Collect Network Traffic Flow Logs | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 13.10 | Perform Application Layer Filtering | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-environment-privil eged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environme nt does not have privileged mode enabled. This setting should be disabled to prevent unintende d access to Docker APIs as well as the container's underlyin g hardware. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| 16.1 | Establish and Maintain a Secure Application Development Process | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16.12 | Implement Code-Level Security Checks | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| 16.12 | Implement Code-Level Security Checks | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16.12 | Implement Code-Level Security Checks | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |
| 16.12 | Implement Code-Level Security Checks | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 16.12 | Implement Code-Level Security Checks | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

### Template

The template is available on GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG3.

## Operational Best Practices for CIS Top 20

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Center for Internet Security (CIS) Top 20 Critical Security Controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CIS Top 20 controls. A CIS Top 20 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the CIS Top 20.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.2 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| CIS.2 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CIS.2 | ec2-security-group-attached-to-eni | This rule ensures the security groups are attached to an Amazon Elastic Compute |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |
| CIS.2 | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organizat ion's standards. |
| CIS.2 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.2 | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| CIS.3 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.3 | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |
| CIS.3 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.4 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CIS.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.4 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| CIS.4 | root-account-hardware-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.4 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CIS.4 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.5 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| CIS.5 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.5 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CIS.5 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.5 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| CIS.6 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| CIS.6 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CIS.6 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CIS.6 | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CIS.6 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| CIS.6 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.6 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| CIS.8 | guardduty-enabled-centraliz ed | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CIS.9 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CIS.9 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| CIS.9 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CIS.9 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within anAmazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| CIS.9 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| CIS.9 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CIS.9 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | s3-account-level-public-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| CIS.9 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CIS.9 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CIS.9 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.9 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| CIS.10 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.10 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| CIS.10 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.10 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CIS.10 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| CIS.11 | ec2-security-group-attached-to-eni | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.11 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| CIS.11 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.11 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| CIS.11 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CIS.12 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CIS.12 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| CIS.12 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CIS.12 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within anAmazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| CIS.12 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| CIS.12 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CIS.12 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | s3-account-level-public-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| CIS.12 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CIS.12 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| CIS.12 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.12 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| CIS.13 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.13 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CIS.13 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| CIS.13 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| CIS.13 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.13 | ec2-ebs-encryption-by-defau lt | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| CIS.13 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CIS.13 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| CIS.13 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.13 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| CIS.13 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CIS.13 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.13 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| CIS.13 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.13 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| CIS.13 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CIS.13 | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.13 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| CIS.13 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CIS.13 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.13 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| CIS.13 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| CIS.14 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CIS.14 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| CIS.14 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| CIS.14 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| CIS.14 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CIS.14 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| CIS.14 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CIS.14 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| CIS.14 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |
| CIS.14 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| CIS.14 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CIS.14 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CIS.14 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| CIS.14 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CIS.14 | s3-account-level-public-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| CIS.14 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| CIS.14 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CIS.14 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| CIS.14 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.14 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| CIS.14 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| CIS.14 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |
| CIS.16 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| CIS.16 | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionall y set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLowercaseCh aracters (AWS Foundatio nal Security Best Practices value: true), RequireSy mbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
|---|---|---|
| | | actual values should reflect your organization's policies. |
| CIS.16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CIS.16 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| CIS.16 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| CIS.16 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| CIS.16 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CIS.16 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| CIS.16 | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.16 | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| CIS.16 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.18 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| CIS.18 | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |
| CIS.19 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.19 | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |
| CIS.19 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CIS.2 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

### Template

The template is available on GitHub: Operational Best Practices for CIS Top 20.

## Operational Best Practices for CISA Cyber Essentials

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity & Infrastructure Security Agency (CISA) Cyber Essentials (CE) and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more CISA CE controls. A CISA CE control can be related to multiple AWS Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Staff-1 | Develop a culture of awareness to encourage employees to make good choices online. | security-awareness-program-exists(Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| Your Staff-2 | Learn about risks like phishing and business email compromise.XXXXX. | security-awareness-program-exists(Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| Your Staff-3 | Maintain awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and | security-awareness-program-exists(Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | agile to cybersecurity trends. | | various security breaches or incidents. |
| Your Staff-4 | Leverage basic cybersecurity training to improve exposure to cybersecurity concepts, terminolo gy and activitie s associated with implementing cybersecurity best practices. | security-awareness -program-exists(Pr ocess Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| Your Staff-5 | Identify available training resources through professio nal associations, academic institutions, private sector and government sources. | security-awareness -program-exists(Pr ocess Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-1 | Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack. | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Your Systems-1 | Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack. | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-1 | Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-1 | Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-1 | Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| Your Systems-1 | Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-1 | Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |
| Your Systems-2 | Leverage automatic updates for all operating systems and third-party software. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-2 | Leverage automatic updates for all operating systems and third-party software. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-2 | Leverage automatic updates for all operating systems and third-party software. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-2 | Leverage automatic updates for all operating systems and third-party software. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | opensearch-data-node-fault-tolerance | Amazon OpenSearch Service (OpenSearch Service) requires at least three data nodes for high availability and fault-tolerance. Deploying an OpenSearch Service domain with at least three data nodes ensures cluster operations if a node fails. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | secretsmanager-secret-periodic-rotation | This rule ensures AWS Secrets Manager secrets have periodic rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Systems-3 | Implement security configurations for all hardware and software assets. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-3 | Implement security configurations for all hardware and software assets. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Systems-4 | Remove unsupported or unauthorized hardware and software from systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-1 | Learn who is on your network. Maintain inventories of network connections (users, vendors, business partners, etc.). | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Your Surroundings-1 | Learn who is on your network. Maintain inventories of network connections (users, vendors, business partners, etc.). | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-1 | Learn who is on your network. Maintain inventories of network connections (users, vendors, business partners, etc.). | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |
| Your Surroundings-2 | Leverage multi-factor authentication for all users, starting with privileged, administrative and remote access users. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-2 | Leverage multi-factor authentication for all users, starting with privileged, administrative and remote access users. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-2 | Leverage multi-factor authentication for all users, starting with privileged, administrative and remote access users. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-2 | Leverage multi-factor authentication for all users, starting with privileged, administrative and remote access users. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-3 | Grant access and admin permissio ns based on need-to-know and least privilege. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-3 | Grant access and admin permissio ns based on need-to-know and least privilege. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Your Surroundings-3 | Grant access and admin permissio ns based on need-to-know and least privilege. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-3 | Grant access and admin permissio ns based on need-to-know and least privilege. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-3 | Grant access and admin permissio ns based on need-to-know and least privilege. | s3-bucket-policy-g rantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_gran tee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principal s, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| Your Surroundings-3 | Grant access and admin permissio ns based on need-to-know and least privilege. | secretsmanager-sec ret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-3 | Grant access and admin permissio ns based on need-to-know and least privilege. | opensearch-access-control-enabled | Ensure fine-grai ned access control is enabled on your Amazon OpenSearc h Service domains. Fine-grained access control provides enhanced authoriza tion mechanisms to achieve least-pri vileged access to Amazon OpenSearc h Service domains. It allows for role-base d access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-ten ancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Surroundings-4 | Leverage unique passwords for all users. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| Your Data-1 | Learn how your data is protected. | kms-cmk-not-schedu led-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-1 | Learn how your data is protected. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Your Data-1 | Learn how your data is protected. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| Your Data-1 | Learn how your data is protected. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Your Data-1 | Learn how your data is protected. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Your Data-1 | Learn how your data is protected. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| Your Data-1 | Learn how your data is protected. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |
| Your Data-1 | Learn how your data is protected. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Your Data-1 | Learn how your data is protected. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Your Data-1 | Learn how your data is protected. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Your Data-1 | Learn how your data is protected. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Your Data-1 | Learn how your data is protected. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-1 | Learn how your data is protected. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Your Data-1 | Learn how your data is protected. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-1 | Learn how your data is protected. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| Your Data-1 | Learn how your data is protected. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-2 | Learn what is happening on your network. manage network and perimeter component s, host and device components, data-at-rest and in-transi t, and user behavior activities. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |
| Your Data-3 | Domain name system protection. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Your Data-4 | Establish regular automated backups and redundancies of key systems. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Your Data-5 | Leverage protections for backups, including physical security, encryption and offline copies. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Data-5 | Leverage protectio ns for backups, including physical security, encryption and offline copies. | backup-recovery-po int-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |
| Your Crisis Response-2 | Lead development of an internal reporting structure to detect, communicate and contain attacks. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Your Crisis Response-2 | Lead development of an internal reporting structure to detect, communicate and contain attacks. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | ebs-optimized-inst ance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contentio n between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | backup-recovery-po int-minimum-retent ion-check | To help with data back-up processes , ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. This rule allows you to set the requiredRetentionD ays (config default: 35) parameter. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | ec2-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-1 | Employ a backup solution that automatically and continuously backs up critical data and system configura tions. | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-2 | Require multi-factor authentication (MFA) for accessing your systems whenever possible.MFA should be required of all users, but start with privileged, administrative, and remote access users. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-2 | Require multi-factor authentication (MFA) for accessing your systems whenever possible.MFA should be required of all users, but start with privileged, administrative, and remote access users. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-2 | Require multi-factor authentication (MFA) for accessing your systems whenever possible.MFA should be required of all users, but start with privileged, administrative, and remote access users. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-2 | Require multi-factor authentication (MFA) for accessing your systems whenever possible.MFA should be required of all users, but start with privileged, administrative, and remote access users. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Booting Up: Things to Do First-3 | Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-3 | Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| Booting Up: Things to Do First-3 | Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| Booting Up: Things to Do First-3 | Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

## Template

The template is available on GitHub: Operational Best Practices for CISA Cyber Essentials.

# Operational Best Practices for Criminal Justice Information Services (CJIS)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Criminal Justice Information Services (CJIS) Compliance Requirements and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CJIS controls. A CJIS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.2 | Security Awareness Training | security-awareness -program-exists (Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| 5.3 | Incident Response | response-plan-exists-maintained (Process Check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel . Having updated and formally documente |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | d response plans can assist in making sure response personnel understand roles, responsibilities and processes to be followed during an incident. |
| 5.3 | Incident Response | response-plan-tested (Process Check) | Ensure Incident response and recovery plans are tested. This can assist in understanding if your plan will be effective during an incident and if any gaps or updates need to be addressed. |
| 5.4 | Auditing and Accountability | audit-log-policy-exists (Process check) | Establish and maintain an audit log management policy that defines your organization's logging requirements. This includes, but is not limited to, review and retention of audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 5.4.1 | Auditable Events and Content (Information Systems) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 5.4.1 | Auditable Events and Content (Information Systems) | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 5.4.1 | Auditable Events and Content (Information Systems) | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |
| 5.4.1 | Auditable Events and Content (Information Systems) | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.4.1 | Auditable Events and Content (Information Systems) | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 5.4.1 | Auditable Events and Content (Information Systems) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 5.4.1 | Auditable Events and Content (Information Systems) | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.1 | Auditable Events and Content (Information Systems) | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| 5.4.5 | Protection of Audit Information | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.5 | Protection of Audit Information | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 5.4.5 | Protection of Audit Information | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.4.6 | Audit Record Retention | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 5.4.6 | Audit Record Retention | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2 | Access Enforcement | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2 | Access Enforcement | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2 | Access Enforcement | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2 | Access Enforcement | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.5.2 | Access Enforcement | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionall y set RequireUp percaseCharacters (CJIS value: false), RequireLowercaseCh aracters (CJIS value: false), RequireSy mbols (CJIS value: false), RequireNu mbers (CJIS value: false), MinimumPa sswordLength (CJIS value: 8), PasswordR eusePrevention (CJIS value: 10), and MaxPasswordAge (CJIS value: 90) for your IAM Password Policy. The actual |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | values should reflect your organization's policies. |
| 5.5.2 | Access Enforcement | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 5.5.2 | Access Enforcement | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.5.2 | Access Enforcement | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 5.5.2 | Access Enforcement | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.5.2 | Access Enforcement | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2 | Access Enforcement | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2 | Access Enforcement | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2 | Access Enforcement | rds-instance-iam-authentication-enabled | Ensure an AWS Identity and Access Management (IAM) authentication is enabled on Amazon Relational Database Service (Amazon RDS) instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). You are not required to store user credentials in the database, as authentication is managed externally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.5.2 | Access Enforcement | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.5.2.1 | Least Privilege | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the containerâ€™s underlying hardware. |
| 5.5.2.1 | Least Privilege | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 5.5.2.1 | Least Privilege | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | ecs-containers-non privileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitio ns should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |
| 5.5.2.1 | Least Privilege | ecs-containers-rea donly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instanceâ €™s filesystem cannot be modified unless it has explicit read-write permissio ns. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| 5.5.2.1 | Least Privilege | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.2.1 | Least Privilege | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.5.6 | Remote Access | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.5.6 | Remote Access | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.6.2.1.1 | Password | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionall y set RequireUp percaseCharacters (CJIS value: false), RequireLowercaseCh aracters (CJIS value: false), RequireSy mbols (CJIS value: false), RequireNu mbers (CJIS value: false), MinimumPa sswordLength (CJIS value: 8), PasswordR eusePrevention (CJIS value: 10), and MaxPasswordAge (CJIS value: 90) for your IAM Password Policy. The actual |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.6.2.2 | Advanced Authentication | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 5.6.2.2 | Advanced Authentication | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.6.2.2 | Advanced Authentication | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.6.2.2 | Advanced Authentication | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.6.2.2 | Advanced Authentication | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.6.3.1 | Identifier Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.7.1.1 | Least Functionality | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 5.7.1.1 | Least Functionality | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 5.7.1.1 | Least Functionality | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.7.1.1 | Least Functionality | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 5.7.1.1 | Least Functionality | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 5.7.1.1 | Least Functionality | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 5.7.1.1 | Least Functionality | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 5.7.1.1 | Least Functionality | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 5.7.1.1 | Least Functionality | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.7.1.1 | Least Functionality | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.7.1.1 | Least Functionality | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 5.7.1.1 | Least Functionality | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10 | System and Communications Protection and Information Integrity | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10 | System and Communications Protection and Information Integrity | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| 5.10 | System and Communications Protection and Information Integrity | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10 | System and Communications Protection and Information Integrity | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |
| 5.10 | System and Communications Protection and Information Integrity | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10 | System and Communications Protection and Information Integrity | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collectio n of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| 5.10.1 | Information Flow Enforcement | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1 | Information Flow Enforcement | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1 | Information Flow Enforcement | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 5.10.1 | Information Flow Enforcement | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10.1 | Information Flow Enforcement | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 5.10.1 | Information Flow Enforcement | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1 | Information Flow Enforcement | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 5.10.1 | Information Flow Enforcement | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10.1 | Information Flow Enforcement | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 5.10.1 | Information Flow Enforcement | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10.1 | Information Flow Enforcement | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 5.10.1 | Information Flow Enforcement | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1 | Information Flow Enforcement | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.1 | Boundary Protection | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1.1 | Boundary Protection | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.1 | Boundary Protection | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| 5.10.1.1 | Boundary Protection | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.1 | Boundary Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.1 | Boundary Protection | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.1 | Boundary Protection | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| 5.10.1.1 | Boundary Protection | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10.1.1 | Boundary Protection | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no condition s could result in unintended behavior. |
| 5.10.1.1 | Boundary Protection | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |
| 5.10.1.1 | Boundary Protection | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collectio n of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1.2 | Encryption | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 5.10.1.2 | Encryption | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| 5.10.1.2 | Encryption | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10.1.2 | Encryption | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 5.10.1.2 | Encryption | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| 5.10.1.2 | Encryption | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |
| 5.10.1.2 | Encryption | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 5.10.1.2 | Encryption | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 5.10.1.2 | Encryption | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1.2 | Encryption | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10.1.2 | Encryption | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 5.10.1.2 | Encryption | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1.2 | Encryption | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| 5.10.1.2 | Encryption | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 5.10.1.2 | Encryption | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1.2 | Encryption | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.10.1.2 | Encryption | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1.2 | Encryption | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 5.10.1.2 | Encryption | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| 5.10.1.2 | Encryption | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 5.10.1.2 | Encryption | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 5.10.1.2 | Encryption | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.2 | Encryption | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 5.10.1.3 | Intrusion Detection Tools and Techniques | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.3 | Intrusion Detection Tools and Techniques | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.1.3 | Intrusion Detection Tools and Techniques | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.4.1 | Patch Management | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.4.1 | Patch Management | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.4.1 | Patch Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.4.1 | Patch Management | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.4.1 | Patch Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 5.10.4.4 | Security Alerts and Advisories | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.4.4 | Security Alerts and Advisories | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.10.4.4 | Security Alerts and Advisories | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

### Template

The template is available on GitHub: Operational Best Practices for CJIS.

## Operational Best Practices for CMMC 2.0 Level 1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard.

You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC 2.0 Level 1 controls. A CMMC 2.0 Level 1 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |
| AC.L1-3.1.1 | Limit information system access to | dms-replication-not-public | Manage access to the AWS Cloud |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | | by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Managemen t (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentia ls. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L1-3.1.20 | Verify and control/limit connections to and use of external information systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| IA.L1-3.5.1 | Identify information system users, processes acting on behalf of users, or devices. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | Authenticate (or verify) the identitie s of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | Authenticate (or verify) the identitie s of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| IA.L1-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA.L1-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L1-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | sagemaker-notebook -no-direct-internet- access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC.L1-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L1-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | opensearch-node-to -node-encryption-c heck | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L1-3.14.1 | Identify, report, and correct informati on and information system flaws in a timely manner. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L1-3.14.1 | Identify, report, and correct informati on and information system flaws in a timely manner. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L1-3.14.1 | Identify, report, and correct informati on and information system flaws in a timely manner. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI.L1-3.14.2 | Provide protection from malicious code at appropriate locations within organizational information systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SI.L1-3.14.5 | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

## Template

The template is available on GitHub: Operational Best Practices for CMMC 2.0 Level 1.

# Operational Best Practices for CMMC 2.0 Level 2

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more CMMC 2.0 Level 2 controls. A CMMC 2.0 Level 2 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | value should reflect your organization's policies. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | secretsmanager-rot ation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | secretsmanager-sch eduled-rotation-su ccess-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.1 | Limit information system access to authorized users, processes acting on behalf of authorize d users, or devices (including other information systems). | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.2 | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.20 | Verify and control/limit connections to and use of external information systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.3 | Control the flow of CUI in accordance with approved authorizations. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC.L2-3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | s3-bucket-policy-g rantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_gran tee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principal s, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | internet-gateway-a uthorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| AC.L2-3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC.L2-3.1.7 | Prevent non-privi leged users from executing privileged functions and capture the execution of such functions in audit logs. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privi leged users from executing privileged functions and capture the execution of such functions in audit logs. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AC.L2-3.1.7 | Prevent non-privi leged users from executing privileged functions and capture the execution of such functions in audit logs. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.7 | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.12 | Monitor and control remote access sessions. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC.L2-3.1.12 | Monitor and control remote access sessions. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AC.L2-3.1.12 | Monitor and control remote access sessions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.12 | Monitor and control remote access sessions. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC.L2-3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitorin g, analysis, investiga tion, and reporting of unlawful or unauthori zed system activity. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.1 | Create and retain system audit logs and records to the extent needed to enable the monitorin g, analysis, investiga tion, and reporting of unlawful or unauthori zed system activity. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU.L2-3.3.2 | Ensure that the actions of individua l system users can be uniquely traced to those users so they can be held accountable for their actions. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU.L2-3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | Ensure that the actions of individua l system users can be uniquely traced to those users so they can be held accountable for their actions. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | Ensure that the actions of individua l system users can be uniquely traced to those users so they can be held accountable for their actions. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | Ensure that the actions of individua l system users can be uniquely traced to those users so they can be held accountable for their actions. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.2 | Ensure that the actions of individua l system users can be uniquely traced to those users so they can be held accountable for their actions. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.4 | Alert in the event of an audit logging process failure. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU.L2-3.3.4 | Alert in the event of an audit logging process failure. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU.L2-3.3.4 | Alert in the event of an audit logging process failure. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.4 | Alert in the event of an audit logging process failure. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.5 | Correlate audit record review, analysis, and reporting processes for investigation and response to indicatio ns of unlawful, unauthorized, suspicious, or unusual activity. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.5 | Correlate audit record review, analysis, and reporting processes for investigation and response to indicatio ns of unlawful, unauthorized, suspicious, or unusual activity. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | cloudwatch-log-gro up-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| AU.L2-3.3.8 | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA.L2-3.12.2 | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsibilities. |
| CA.L2-3.12.3 | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA.L2-3.12.3 | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA.L2-3.12.3 | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM.L2-3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CM.L2-3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |
| CM.L2-3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | account-part-of-or ganizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsist ent account configura tions, which may expose resources and sensitive data. |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | ec2-instance-manag ed-by-systems-mana ger | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | ec2-managedinstanc e-association-comp liance-status-check | Use AWS Systems Manager Associati ons to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configura tion state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configura tions, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | ec2-managedinstanc e-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | elastic-beanstalk-managed-updates-en abled | Enabling managed platform updates for an Amazon Elastic Beanstalk environme nt ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | rds-automatic-mino r-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed , which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.2 | Establish and enforce security configuration settings for informati on technology products employed in organizational systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| CM.L2-3.4.3 | Track, review, approve, or disapprov e, and log changes to organizational systems. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprov e, and log changes to organizational systems. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.3 | Track, review, approve, or disapprove, and log changes to organizational systems. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | autoscaling-launch -config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-instance-manag ed-by-systems-mana ger | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-managedinstanc e-association-comp liance-status-check | Use AWS Systems Manager Associati ons to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configura tion state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configura tions, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | internet-gateway-a uthorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | no-unrestricted-ro ute-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.7 | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.9 | Control and monitor user-installed software. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.9 | Control and monitor user-installed software. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM.L2-3.4.9 | Control and monitor user-installed software. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| IA.L2-3.5.1 | Identify information system users, processes acting on behalf of users, or devices. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.1 | Identify informati on system users, processes acting on behalf of users, or devices. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.2 | Authenticate (or verify) the identitie s of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| IA.L2-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA.L2-3.5.2 | Authenticate (or verify) the identitie s of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentia ls. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA.L2-3.5.3 | Use multifactor authentication for local and network access to privilege d accounts and for network access to non-privileged accounts. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.6 | Disable identifiers after a defined period of inactivity. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.6 | Disable identifiers after a defined period of inactivity. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.7 | Enforce a minimum password complexit y and change of characters when new passwords are created. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.8 | Prohibit password reuse for a specified number of generatio ns. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | alb-http-drop-inva lid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | elasticsearch-encr ypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| IA.L2-3.5.10 | Store and transmit only cryptogra phically-protected passwords. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| IA.L2-3.5.10 | Store and transmit only cryptographically-protected passwords. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR.L2-3.6.1 | Establish an operational incident-handling capabilit y for organizat ional systems that includes preparati on, detection, analysis, containme nt, recovery, and user response activities. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR.L2-3.6.1 | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR.L2-3.6.1 | Establish an operational incident-handling capabilit y for organizat ional systems that includes preparati on, detection, analysis, containme nt, recovery, and user response activities. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR.L2-3.6.1 | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| IR.L2-3.6.3 | Test the organizational incident response capability. | response-plan-tested (Process Check) | Ensure Incident response and recovery plans are tested. This can assist in understanding if your plan will be effective during an incident and if any gaps or updates need to be addressed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| MA.L2-3.7.5 | Require multifact or authentication to establish nonlocal maintenance sessions from external network connections and terminate such connections when nonlocal maintenan ce is complete. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| MA.L2-3.7.5 | Require multifact or authentication to establish nonlocal maintenance sessions from external network connections and terminate such connections when nonlocal maintenan ce is complete. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Managemen t (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentia ls. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA.L2-3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| RA.L2-3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA.L2-3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA.L2-3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizat ional communica tions (i.e., informati on transmitted or received by organizat ional information systems) at the external boundarie s and key internal boundaries of the information systems. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.1 | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | autoscaling-launch -config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | dynamodb-autoscali ng-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/writ e capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | elb-deletion-prote ction-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| SC.L2-3.13.4 | Prevent unauthori zed and unintended information transfer from shared system resources. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC.L2-3.13.4 | Prevent unauthori zed and unintended information transfer from shared system resources. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.4 | Prevent unauthorized and unintended information transfer from shared system resources. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC.L2-3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.10 | Establish and manage cryptographic keys for cryptography employed in organizational systems. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC.L2-3.13.10 | Establish and manage cryptographic keys for cryptography employed in organizational systems. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| SC.L2-3.13.15 | Protect the authenticity of communications sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.15 | Protect the authenticity of communications sessions. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| SC.L2-3.13.15 | Protect the authenticity of communications sessions. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.15 | Protect the authenticity of communications sessions. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC.L2-3.13.15 | Protect the authenticity of communications sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.15 | Protect the authenticity of communications sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| SC.L2-3.13.16 | Protect the confidentiality of CUI at rest. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI.L2-3.14.1 | Identify, report, and correct informati on and information system flaws in a timely manner. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.1 | Identify, report, and correct informati on and information system flaws in a timely manner. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.1 | Identify, report, and correct informati on and information system flaws in a timely manner. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.2 | Provide protection from malicious code at appropriate locations within organizational information systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SI.L2-3.14.5 | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.3 | Monitor system security alerts and advisories and take action in response. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| SI.L2-3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI.L2-3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI.L2-3.14.7 | Identify unauthorized use of organizational systems. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

### Template

The template is available on GitHub: Operational Best Practices for CMMC 2.0 Level 2.

## Operational Best Practices for Compute Services

This conformance pack contains AWS Config rules based on Compute Services. For more information, see Compute for any workload. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Compute Services.

## Operational Best Practices for Data Resiliency

For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Data Resiliency.

## Operational Best Practices for Databases Services

This conformance pack contains AWS Config rules based on Databases Services. For more information, see Databases on AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Databases Services.

## Operational Best Practices for Data Lakes and Analytics Services

This conformance pack contains AWS Config rules for Data Lakes and Analytics Services. For more information, see Data Lakes and Analytics on AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Data Lakes and Analytics Services.

## Operational Best Practices for DevOps

This conformance pack contains AWS Config rules based on DevOps within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for DevOps.

## Operational Best Practices for EC2

This conformance pack contains AWS Config rules based on EC2. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for EC2.

## Operational Best Practices for Encryption and Key Management

For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Encryption and Key Management.

## Operational Best Practices for ENISA Cybersecurity guide for SMEs

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the European Union Agency for Cybersecurity (ENISA) Cybersecurity guide for SMEs and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more ENISA Cybersecurity guide for SMEs controls. An ENISA Cybersecurity guide for SMEs control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls adapted from the ENISA Cybersecurity guide for SMEs. The ENISA Cybersecurity guide for SMEs is available at Cybersecurity guide for SMEs - 12 steps to securing your business.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: PUBLISH CYBERSECURITY POLICIES | Clear and specific rules should be outlined in cybersecurity | security-awareness-program-exists(Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | | cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-bucket-level-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-bucket-acl-proh ibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | alb-http-drop-inva lid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | api-gw-cache-enabl ed-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | backup-recovery-point-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | dynamodb-table-enc rypted-kms | Ensure that encryptio n is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | elasticsearch-encr ypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elasticsearch Service (Amazon ES) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | efs-access-point-e nforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirect ory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | efs-access-point-e nforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configure d on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | cloudwatch-log-gro up-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | secretsmanager-usi ng-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | opensearch-encrypt ed-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | elasticsearch-node-to-node-encryption-check | Ensure node-to-n ode encryption for Amazon Elasticse arch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | opensearch-node-to -node-encryption-c heck | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | kinesis-stream-enc rypted | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | internet-gateway-a uthorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | no-unrestricted-ro ute-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | rds-snapshot-encry pted | Ensure that encryptio n is enabled for your Amazon Relationa l Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | rds-storage-encryp ted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-bucket-server-s ide-encryption-ena bled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION | Under the EU General Data Protection Regulation1 any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate securi ty controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2_PROVIDE APPROPRIATE TRAINING | Provide regular cybersecurity awareness trainings for all employees to ensure they can recognize and deal with the various cybersecurity threats. These trainings should be tailored for SME's and focus on real-life situations. Provide specialized cybersecurity training for those responsible for managing cybersecurity within the business to ensure they will have the skills and competencies required to do their job. | security-awareness-program-exists(Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4_DEVELOP AN INCIDENT RESPONSE PLAN | Develop a formal incident response plan, which contains clear guidelines, roles and responsibiliti es documented to ensure that all security incidents are responded to in a timely, professio nal and appropria te manner. To respond quickly to security threats, investigate tools that could monitor and create alerts when suspicious activity or security breaches are occurring. | response-plan-exists-maintained(Process Check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel . |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5_SECURE ACCESS TO SYSTEMS | Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security. If you opt for a typical password: - Make it long, with lower and upper case characters, possibly also numbers and special characters. - Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”. - Avoid using personal info that can be found online. And whether you use passphrases or passwords - Do not reuse them elsewhere. - Do not share them with colleagues. - Enable Multi-Factor Authentication. - Use | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | a dedicated password manager. | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5_SECURE ACCESS TO SYSTEMS | Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security. If you opt for a typical password: - Make it long, with lower and upper case characters, possibly also numbers and special characters. - Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”. - Avoid using personal info that can be found online. And whether you use passphrases or passwords - Do not reuse them elsewhere. - Do not share them with colleagues. - Enable Multi-Factor Authentication. - Use | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | a dedicated password manager. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5_SECURE ACCESS TO SYSTEMS | Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security. If you opt for a typical password: - Make it long, with lower and upper case characters, possibly also numbers and special characters. - Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”. - Avoid using personal info that can be found online. And whether you use passphrases or passwords - Do not reuse them elsewhere. - Do not share them with colleagues. - Enable Multi-Factor Authentication. - Use | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | a dedicated password manager. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5_SECURE ACCESS TO SYSTEMS | Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security. If you opt for a typical password: - Make it long, with lower and upper case characters, possibly also numbers and special characters. - Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”. - Avoid using personal info that can be found online. And whether you use passphrases or passwords - Do not reuse them elsewhere. - Do not share them with colleagues. - Enable Multi-Factor Authentication. - Use | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | a dedicated password manager. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5_SECURE ACCESS TO SYSTEMS | Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security. If you opt for a typical password: - Make it long, with lower and upper case characters, possibly also numbers and special characters. - Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”. - Avoid using personal info that can be found online. And whether you use passphrases or passwords - Do not reuse them elsewhere. - Do not share them with colleagues. - Enable Multi-Factor Authentication. - Use | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | a dedicated password manager. | | |
| 6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE | Ideally using a centralized platform to manage patching. It is highly re commended for SMEs to: - Regularly update all of their software. - Turn on automatic updates whenever possible. - Identify software and hardware that requires manual updates. - Take into account mobile and IoT devices. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE | Ideally using a centralized platform to manage patching. It is highly re commended for SMEs to: - Regularly update all of their software. - Turn on automatic updates whenever possible. - Identify software and hardware that requires manual updates. - Take into account mobile and IoT devices. | ec2-managedinstanc e-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE | Ideally using a centralized platform to manage patching. It is highly re commended for SMEs to: - Regularly update all of their software. - Turn on automatic updates whenever possible. - Identify software and hardware that requires manual updates. - Take into account mobile and IoT devices. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE | Ideally using a centralized platform to manage patching. It is highly re commended for SMEs to: - Regularly update all of their software. - Turn on automatic updates whenever possible. - Identify software and hardware that requires manual updates. - Take into account mobile and IoT devices. | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE | Ideally using a centralized platform to manage patching. It is highly re commended for SMEs to: - Regularly update all of their software. - Turn on automatic updates whenever possible. - Identify software and hardware that requires manual updates. - Take into account mobile and IoT devices. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environme nt ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE | Ideally using a centralized platform to manage patching. It is highly re commended for SMEs to: - Regularly update all of their software. - Turn on automatic updates whenever possible. - Identify software and hardware that requires manual updates. - Take into account mobile and IoT devices. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed , which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE | Ideally using a centralized platform to manage patching. It is highly re commended for SMEs to: - Regularly update all of their software. - Turn on automatic updates whenever possible. - Identify software and hardware that requires manual updates. - Take into account mobile and IoT devices. | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | opensearch-encrypt ed-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | sagemaker-endpoint -configuration-kms- key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | sagemaker-notebook -instance-kms-key- configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferr ed over public networks, such as hotel or airport WiFi networks, ensure th at data is encrypted , either by employ ing a Virtual Private Network (VPN) or accessing websites over secure connectio ns using SSL/TLS p rotocol. Ensure their own websites are employing suitable encryption technol ogy to protect client data as it travels over the Internet. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6_SECURE DEVICES: ENCRYPTION | Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | netfw-policy-rule-group-associated | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows, and you define default traffic handling. |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | netfw-stateless-rule-group-not-empty | An AWS Network Firewall rule group contains rules that define how your firewall processes traffic in your VPC. An empty stateless rule group when present in a firewall policy does not process traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no condition s could result in unintended behavior. |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: EMPLOY FIREWALLS | Firewalls manage the traffic that enters and leaves a network a nd are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particula r a firewall should be employed to protect the SME's network f rom the Internet. | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collectio n of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Managemen t (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentia ls. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentia ls. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | elasticsearch-logs-to-cloudwatch | Ensure Amazon Elasticsearch service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS | SMEs should regularly review any remote access tools to ensure they are secure, particularly: - Ensure all remote access software is patched and up date. - Restrict remote access from suspiciou s geographical locat ions or certain IP addresses. - Restrict staff remote access only to the systems and computers they need for their work. - Enforce strong passwords for remote access and where pos sible enable multi-fac tor authentication. - Ensure monitorin g and alerting is enabled to warn of suspected attacks or unusual suspicious activity. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | backup-recovery-po int-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | backup-recovery-po int-minimum-retent ion-check | To help with data back-up processes , ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. This rule allows you to set the requiredRetentionD ays (config default: 35) parameter. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups should be maintained as they are an effective way to recover from disasters such as a ransomware attack. The following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's production environment, - backups are encrypted, especially if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | rds-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 9_SECURE BACKUPS | To enable the recovery of key formation, backups s hould be maintaine d as they are an effective way to recover from disasters such as a ransomware attack. T he following backup rules should apply: - backup is regular and automated whenever possible, - backup is held separately from the SME's pro duction environme nt, - backups are encrypted, especiall y if they are going to be moved between locations, - the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11_SECURE ONLINE SITES | It is essential that SMEs ensure that their online websites are configured and maintained in a secure manner an d that any personal data or financial details, such as credit card data, is appropriately protected. This will entail running regular security tests against the websites to identify any potential security weaknesse s and conductin g regular reviews to ensure the site is maintained and updated properly. | vuln-management-plan-exists(Process Check) | Ensure a vulnerabi lity management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. |

### Template

The template is available on GitHub: Operational Best Practices for ENISA Cybersecurity guide for SMEs.

## Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates,

are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Spain Esquema Nacional de Seguridad (ENS) Low framework controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more Spain ENS Low controls. A Spain ENS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the Spain ENS Low framework, as last updated on 2020/10/23.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Anexo II 4.1.2.a); b); c) | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| Anexo II 4.1.2.a); b); c) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Anexo II 4.1.2.a); b); c) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 4.1.2.a); b); c) | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Anexo II 4.1.2.a); b); c) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Anexo II 4.1.2.a); b); c) | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Anexo II 4.1.2.a); b); c) | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Anexo II 4.1.2.a); b); c) | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 4.1.2.a); b); c) | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Anexo II 4.1.2.a); b); c) | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Anexo II 4.1.2.a); b); c) | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Anexo II 4.1.2.b) | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| Anexo II 4.1.2.b) | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| Anexo II 4.1.2.b) | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Anexo II 4.1.2.b) | vpc-network-acl-unused-chec k | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitorin g for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.1.a) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| Anexo II 4.2.1.a); b) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.4 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| Anexo II 4.2.4 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Anexo II 4.2.4 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.a) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.c) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
|---|---|---|
| | | actual values should reflect your organization's policies. |
| Anexo II 4.2.6.BAJO.c) | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.2.6.BAJO.c) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| Anexo II 4.2.6.BAJO.c) | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Anexo II 4.2.6.BAJO.c) | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| Anexo II 4.2.6.BAJO.c) | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| Anexo II 4.2.6.BAJO.c) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.7.BAJO | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| Anexo II 4.2.7.BAJO | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.7.BAJO | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Anexo II 4.2.7.BAJO | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| Anexo II 4.3.1 | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| Anexo II 4.3.1 | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Anexo II 4.3.1 | vpc-network-acl-unused-chec k | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitorin g for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| Anexo II 4.3.2.b) | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Anexo II 4.3.2.b) | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestric ted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| Anexo II 4.3.2.b) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| Anexo II 4.3.2.b) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| Anexo II 4.3.2.b) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| Anexo II 4.3.2.b) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| Anexo II 4.3.2.b) | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| Anexo II 4.3.2.b) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| Anexo II 4.3.2.b) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| Anexo II 4.3.2.b) | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Anexo II 4.3.2.b) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Anexo II 4.3.2.b) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| Anexo II 4.3.2.b) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| Anexo II 4.3.4.c) | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsibilities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.3.8.BAJO | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| Anexo II 4.3.8.BAJO | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Anexo II 4.3.8.BAJO | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| Anexo II 4.3.8.BAJO | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Anexo II 4.3.8.BAJO | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| Anexo II 4.3.8.BAJO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| Anexo II 4.3.8.BAJO | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| Anexo II 4.3.10.b) | cloud-trail-encryption-enab led | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.10.b) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Anexo II 4.3.10.d) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.6.1 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Anexo II 4.6.2.BASICA | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.2.3 | security-awareness-program-exists (Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organizat ion from various security breaches or incidents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.3.BAJO.a) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| Anexo II 5.6.1.c) | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| Anexo II 5.6.1.c) | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Anexo II 5.7.3 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 5.7.3 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| Anexo II 5.7.3 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Anexo II 5.7.3 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Anexo II 5.7.3 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 5.7.3 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Anexo II 5.7.3 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| Anexo II 5.7.3 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| Anexo II 5.7.3 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| Anexo II 5.7.4 | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.4 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| Anexo II 5.8.2 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.2 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| Art. 14.4 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 16 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| Art. 16 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Art. 16 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 20.2 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| Art. 20.2 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| Art. 20.2 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 20.2 | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsib ilities. |
| Art. 21.1 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Art. 21.1 | ec2-ebs-encryption-by-defau lt | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| Art. 21.1 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Art. 21.1 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Art. 21.1 | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Art. 21.1 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Art. 21.1 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Art. 21.1 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Art. 21.1 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Art. 21.1 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Art. 21.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Art. 21.1 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Art. 21.1 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Art. 21.1 | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Art. 21.1 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Art. 21.1 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| Art. 21.1 | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Art. 21.1 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Art. 21.1 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Art. 22 | autoscaling-launch-config-p ublic-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Art. 22 | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| Art. 22 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| Art. 22 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| Art. 22 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| Art. 22 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| Art. 22 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| Art. 22 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| Art. 22 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| Art. 22 | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Art. 22 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Art. 22 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| Art. 22 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| Art. 23 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Art. 23 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Art. 23 | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Art. 23 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Art. 23 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Art. 23 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Art. 23 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| Art. 25 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Art. 25 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |
| Art. 25 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| Art. 25 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| Art. 25 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| Art. 25 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

## Template

The template is available on GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low.

# Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Spain Esquema Nacional de Seguridad (ENS) Medium framework controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more Spain ENS Medium controls. A Spain ENS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the Spain ENS Medium framework, as last updated on 2020/10/23.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Anexo II 4.1.2.a); b); c) | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | rds-instance-deletion-prote ction-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Anexo II 4.1.2.a); b); c) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 4.1.2.a); b); c) | cloud-trail-encryption-enab led | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |
| Anexo II 4.1.2.a); b); c) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Anexo II 4.1.2.a); b); c) | cloudwatch-log-group-encryp ted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| Anexo II 4.1.2.a); b); c) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Anexo II 4.1.2.a); b); c) | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 4.1.2.a); b); c) | elb-deletion-protection-ena bled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Anexo II 4.1.2.a); b); c) | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Anexo II 4.1.2.a); b); c) | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Anexo II 4.1.2.b) | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| Anexo II 4.1.2.b) | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| Anexo II 4.1.2.b) | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Anexo II 4.1.2.b) | vpc-network-acl-unused-chec k | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitorin g for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.1.a) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| Anexo II 4.2.1.a); 4.2.1.b) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.4 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| Anexo II 4.2.4 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Anexo II 4.2.4 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5.a) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5.c) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| Anexo II 4.2.6.BAJO.c) | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.2.6.c) | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.c) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Anexo II 4.2.6.c) | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.c) | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Anexo II 4.2.6.c) | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Anexo II 4.2.6.c) | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.c) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Anexo II 4.2.6.c) | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Anexo II 4.2.6.c) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.c) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| Anexo II 4.2.6.c) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.7 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| Anexo II 4.2.7 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.7 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Anexo II 4.2.7 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Anexo II 4.3.1 | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| Anexo II 4.3.1 | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| Anexo II 4.3.1 | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Anexo II 4.3.1 | vpc-network-acl-unused-chec k | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitorin g for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| Anexo II 4.3.2.b) | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| Anexo II 4.3.2.b) | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestric ted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| Anexo II 4.3.2.b) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| Anexo II 4.3.2.b) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| Anexo II 4.3.2.b) | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| Anexo II 4.3.2.b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Anexo II 4.3.2.b) | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| Anexo II 4.3.2.b) | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| Anexo II 4.3.2.b) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| Anexo II 4.3.2.b) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| Anexo II 4.3.2.b) | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Anexo II 4.3.2.b) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Anexo II 4.3.2.b) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| Anexo II 4.3.2.b) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| Anexo II 4.3.4.c) | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsibilities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.6 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Anexo II 4.3.7.a) | response-plan-exists-maintained (Process Check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel. Having updated and formally documented response plans can assist in making sure response personnel understand roles, responsibilities and processes to be followed during an incident. |
| Anexo II 4.3.8 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Anexo II 4.3.8 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Anexo II 4.3.8 | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Anexo II 4.3.8 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Anexo II 4.3.8 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Anexo II 4.3.8 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| Anexo II 4.3.8 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.3.8.MEDIO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.3.10.b) | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.10.b) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Anexo II 4.3.10.d) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.6.1 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Anexo II 4.6.2 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.6.2 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Anexo II 5.2.3 | security-awareness-program-exists (Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| Anexo II 5.4.2 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.2 | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 5.4.2 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.2 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.2 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.2 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 5.4.2 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.2 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.2.MEDIO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 5.4.3 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3 | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.3 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 5.4.3 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.3 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3.MEDIO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.3.a) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| Anexo II 5.6.1.c) | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| Anexo II 5.6.1.c) | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Anexo II 5.7.3 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 5.7.3 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| Anexo II 5.7.3 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Anexo II 5.7.3 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Anexo II 5.7.3 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 5.7.3 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Anexo II 5.7.3 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| Anexo II 5.7.3 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| Anexo II 5.7.3 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| Anexo II 5.7.4 | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.4 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| Anexo II 5.8.2 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.2 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| Anexo II 5.8.3.b) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.b) | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| Anexo II 5.8.3.b) | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.b) | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Anexo II 5.8.3.b) | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| Anexo II 5.8.3.b) | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.b) | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.b) | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.b) | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Art. 14.4 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 16 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| Art. 16 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Art. 16 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 20.2 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| Art. 20.2 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| Art. 20.2 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 20.2 | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsib ilities. |
| Art. 21.1 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Art. 21.1 | ec2-ebs-encryption-by-defau lt | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| Art. 21.1 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Art. 21.1 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Art. 21.1 | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Art. 21.1 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Art. 21.1 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Art. 21.1 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Art. 21.1 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Art. 21.1 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Art. 21.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Art. 21.1 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Art. 21.1 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Art. 21.1 | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Art. 21.1 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Art. 21.1 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| Art. 21.1 | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Art. 21.1 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Art. 21.1 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Art. 22 | autoscaling-launch-config-p ublic-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| Art. 22 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| Art. 22 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| Art. 22 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| Art. 22 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Art. 22 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| Art. 22 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| Art. 22 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| Art. 22 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| Art. 22 | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Art. 22 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Art. 22 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| Art. 22 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| Art. 23 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Art. 23 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Art. 23 | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Art. 23 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Art. 23 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Art. 23 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Art. 23 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| Art. 24.1 | guardduty-enabled-centraliz ed | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Art. 24.2 | response-plan-exists-mainta ined (Process Check) | Ensure incident response plans are established, maintained, and distribut ed to responsible personnel. Having updated and formally documented response plans can assist in making sure response personnel understan d roles, responsibilities and processes to be followed during an incident. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Art. 25 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Art. 25 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| Art. 25 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| Art. 25 | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| Art. 25 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

### Template

The template is available on GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium.

## Operational Best Practices for Esquema Nacional de Seguridad (ENS) High

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Spain Esquema Nacional de Seguridad (ENS) High framework controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more Spain ENS High controls. A Spain ENS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the Spain ENS High framework, as last updated on 2021/07/09.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.1.ALTO | annual-risk-assessment-performed (Process check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting an organization. |
| 4.2.1.b) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 4.2.5.ALTO.a) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | incorporate the principle of least functionality. |
| Anexo II 4.1.2.a); b); c) | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Anexo II 4.1.2.a); b); c) | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| Anexo II 4.1.2.a); b); c) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Anexo II 4.1.2.a); b); c) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 4.1.2.a); b); c) | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Anexo II 4.1.2.a); b); c) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Anexo II 4.1.2.a); b); c) | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Anexo II 4.1.2.a); b); c) | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Anexo II 4.1.2.a); b); c) | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 4.1.2.a); b); c) | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Anexo II 4.1.2.a); b); c) | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Anexo II 4.1.2.a); b); c) | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 4.1.2.a); b); c) | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Anexo II 4.1.2.a); b); c) | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.a); b); c) | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Anexo II 4.1.2.b) | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| Anexo II 4.1.2.b) | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.1.2.b) | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| Anexo II 4.1.2.b) | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Anexo II 4.1.2.b) | vpc-network-acl-unused-chec k | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitorin g for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.1.a) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| Anexo II 4.2.4 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| Anexo II 4.2.4 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.4 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Anexo II 4.2.4 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.a) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.5.BAJO.c) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| Anexo II 4.2.6.ALTO.b) | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| Anexo II 4.2.6.ALTO.b) | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.ALTO.b) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Anexo II 4.2.6.ALTO.b) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Anexo II 4.2.6.BAJO.c) | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Anexo II 4.2.6.BAJO.c) | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Anexo II 4.2.6.BAJO.c) | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Anexo II 4.2.6.BAJO.c) | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Anexo II 4.2.6.BAJO.c) | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Anexo II 4.2.6.BAJO.c) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.2.6.BAJO.c) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.6.BAJO.c) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| Anexo II 4.2.7.BAJO | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.7.BAJO | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| Anexo II 4.2.7.BAJO | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.2.7.BAJO | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| Anexo II 4.3.1 | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| Anexo II 4.3.1 | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.1 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| Anexo II 4.3.1 | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| Anexo II 4.3.1 | vpc-network-acl-unused-chec k | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitorin g for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| Anexo II 4.3.2.b) | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Anexo II 4.3.2.b) | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestric ted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| Anexo II 4.3.2.b) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| Anexo II 4.3.2.b) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| Anexo II 4.3.2.b) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| Anexo II 4.3.2.b) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| Anexo II 4.3.2.b) | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| Anexo II 4.3.2.b) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| Anexo II 4.3.2.b) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| Anexo II 4.3.2.b) | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Anexo II 4.3.2.b) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Anexo II 4.3.2.b) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| Anexo II 4.3.2.b) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.2.b) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| Anexo II 4.3.4.c) | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsibilities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.6 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Anexo II 4.3.7.MEDIA.a) | response-plan-exists-maintained (Process Check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel. Having updated and formally documented response plans can assist in making sure response personnel understand roles, responsibilities and processes to be followed during an incident. |
| Anexo II 4.3.8.BAJO | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Anexo II 4.3.8.BAJO | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Anexo II 4.3.8.BAJO | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Anexo II 4.3.8.BAJO | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Anexo II 4.3.8.BAJO | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Anexo II 4.3.8.BAJO | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.3.8.BAJO | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.BAJO | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| Anexo II 4.3.8.MEDIO | elasticsearch-logs-to-cloud watch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Anexo II 4.3.8.MEDIO | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Anexo II 4.3.8.MEDIO | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Anexo II 4.3.8.MEDIO | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Anexo II 4.3.8.MEDIO | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Anexo II 4.3.8.MEDIO | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 4.3.8.MEDIO | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.8.MEDIO | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| Anexo II 4.3.10.b) | cloud-trail-encryption-enab led | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |
| Anexo II 4.3.10.b) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.3.10.d) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| Anexo II 4.6.1 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.6.2.ALTO | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |
| Anexo II 4.6.2.BASICA | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 4.6.2.MEDIA | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| Anexo II 5.2.3 | security-awareness-program-exists (Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| Anexo II 5.2.4 | security-awareness-program-exists (Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.2.5 | security-awareness-program-exists (Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organizat ion from various security breaches or incidents. |
| Anexo II 5.4.2.MEDIO | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.2.MEDIO | elbv2-acm-certificate-requi red | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.2.MEDIO | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.2.MEDIO | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.2.MEDIO | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 5.4.2.MEDIO | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.2.MEDIO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 5.4.2.MEDIO | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.2.MEDIO | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.3.BAJO.a) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| Anexo II 5.4.3.MEDIO | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3.MEDIO | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 5.4.3.MEDIO | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.3.MEDIO | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3.MEDIO | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 5.4.3.MEDIO | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.4.3.MEDIO | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Anexo II 5.4.3.MEDIO | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.4.3.MEDIO | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.6.1.c) | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| Anexo II 5.6.1.c) | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Anexo II 5.7.3 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
|---|---|---|
| Anexo II 5.7.3 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| Anexo II 5.7.3 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Anexo II 5.7.3 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| Anexo II 5.7.3 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Anexo II 5.7.3 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Anexo II 5.7.3 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Anexo II 5.7.3 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Anexo II 5.7.3 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| Anexo II 5.7.3 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Anexo II 5.7.3 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| Anexo II 5.7.3 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.3 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Anexo II 5.7.3 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| Anexo II 5.7.4 | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.7.4 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| Anexo II 5.8.2 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.2 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| Anexo II 5.8.3.MEDIO.b) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| Anexo II 5.8.3.MEDIO.b) | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Anexo II 5.8.3.MEDIO.b) | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| Anexo II 5.8.3.MEDIO.b) | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Anexo II 5.8.3.MEDIO.b) | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Art. 14.4 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 16 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| Art. 16 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 16 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Art. 16 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 20.2 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| Art. 20.2 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| Art. 20.2 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 20.2 | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsib ilities. |
| Art. 21.1 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Art. 21.1 | ec2-ebs-encryption-by-defau lt | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| Art. 21.1 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| Art. 21.1 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Art. 21.1 | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Art. 21.1 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Art. 21.1 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Art. 21.1 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| Art. 21.1 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| Art. 21.1 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Art. 21.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Art. 21.1 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Art. 21.1 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Art. 21.1 | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| Art. 21.1 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Art. 21.1 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| Art. 21.1 | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| Art. 21.1 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Art. 21.1 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| Art. 21.1 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 21.1 | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| Art. 22 | autoscaling-launch-config-p ublic-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Art. 22 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| Art. 22 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| Art. 22 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| Art. 22 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| Art. 22 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| Art. 22 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| Art. 22 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| Art. 22 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| Art. 22 | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Art. 22 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Art. 22 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| Art. 22 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 22 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| Art. 23 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Art. 23 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Art. 23 | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Art. 23 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Art. 23 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Art. 23 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Art. 23 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 23 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| Art. 24.2 | response-plan-exists-mainta ined (Process Check) | Ensure incident response plans are established, maintained, and distribut ed to responsible personnel. Having updated and formally documented response plans can assist in making sure response personnel understan d roles, responsibilities and processes to be followed during an incident. |
| Art. 24.1 | guardduty-enabled-centraliz ed | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Art. 25 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Art. 25 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| Art. 25 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| Art. 25 | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| Art. 25 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Art. 25 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

### Template

The template is available on GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) High.

## Operational Best Practices for FDA Title 21 CFR Part 11

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Title 21 of the Code of Federal Regulations (CFR) Part 11 and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more FDA Title 21 CFR Part 11 controls. A FDA Title 21 CFR Part 11 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | | s your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.1 | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | dynamodb-autoscali ng-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/writ e capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performan ce, and the ability to discern invalid or altered records. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(a) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | ecr-private-lifecycle-policy-configured | Amazon Elastic Container Repository (ECR) lifecycle policies enable you to specify the lifecycle management of images in a repository. This allows the automation of cleaning up unused images, such as expiring images based on age or count. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(c) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (d) Limiting system access to authorized individuals. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(d) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (d) Limiting system access to authorized individuals. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(e) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (e) Use of secure, computer-generated, time-stam ped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previousl y recorded informati on. Such audit trail | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(g) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (g) Use of authority checks to ensure that only authorize d individuals can use the system, electroni cally sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(h) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (h) Use of device (for example, terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(h) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (h) Use of device (for example, terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(h) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (h) Use of device (for example, terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(i) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following : (i) Determination that persons who develop, maintain, or use electronic record/ electronic signature systems have the education, training, and experience to perform their assigned tasks. | security-awareness -program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documenta tion. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropria te controls over systems documenta tion including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.10(k) | Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | trail that documents time-sequenced development and modification of systems documentation. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlle | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d system access, each signing shall be executed using all of the electronic signature component s. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collabora tion of two or more individuals. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlle | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | d system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlle | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d system access, each signing shall be executed using all of the electronic signature component s. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collabora tion of two or more individuals. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2 | (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlle | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d system access, each signing shall be executed using all of the electronic signature component s. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collabora tion of two or more individuals. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlle | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d system access, each signing shall be executed using all of the electronic signature component s. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collabora tion of two or more individuals. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlle | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d system access, each signing shall be executed using all of the electronic signature component s. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collabora tion of two or more individuals. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.2 | (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlle | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d system access, each signing shall be executed using all of the electronic signature component s. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collabora tion of two or more individuals. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | cloudwatch-log-gro up-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | cmk-backing-key-ro tation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | dynamodb-table-enc rypted-kms | Ensure that encryptio n is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | elasticsearch-encr ypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | opensearch-encrypt ed-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | rds-storage-encryp ted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | sagemaker-endpoint -configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | sagemaker-notebook -instance-kms-key- configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | secretsmanager-usi ng-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.3 | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authentic ity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropria te, and additiona l measures such as document encryption and use of appropria te digital signature standards to ensure, as necessary under the circumstances, record authentic ity, integrity, and confidentiality. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(b) | Persons who use electronic signature s based upon use of identification codes in combinati on with passwords shall employ controls to ensure their security and integrity . Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging). | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(b) | Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging). | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(b) | Persons who use electronic signature s based upon use of identification codes in combinati on with passwords shall employ controls to ensure their security and integrity . Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging). | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(b) | Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging). | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(b) | Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging). | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(b) | Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (for example, to cover such events as password aging). | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(d) | Persons who use electronic signature s based upon use of identification codes in combinati on with passwords shall employ controls to ensure their security and integrity . Such controls shall include: (d) Use of transacti on safeguards to prevent unauthori zed use of passwords and/or identific ation codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(d) | Persons who use electronic signature s based upon use of identification codes in combinati on with passwords shall employ controls to ensure their security and integrity . Such controls shall include: (d) Use of transacti on safeguards to prevent unauthori zed use of passwords and/or identific ation codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.300(d) | Persons who use electronic signature s based upon use of identification codes in combinati on with passwords shall employ controls to ensure their security and integrity . Such controls shall include: (d) Use of transacti on safeguards to prevent unauthori zed use of passwords and/or identific ation codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.300(d) | Persons who use electronic signature s based upon use of identification codes in combinati on with passwords shall employ controls to ensure their security and integrity . Such controls shall include: (d) Use of transacti on safeguards to prevent unauthori zed use of passwords and/or identific ation codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

## Template

The template is available on GitHub: Operational Best Practices for FDA Title 21 CFR Part 11.

# Operational Best Practices for FedRAMP(Low)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Risk and Authorization Management Program (FedRAMP) Low Baseline Controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FedRAMP controls. A FedRAMP control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| AC-2 | ACCOUNT MANAGEMENT | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| AC-2 | ACCOUNT MANAGEMENT | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |
| AC-2 | ACCOUNT MANAGEMENT | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-2 | ACCOUNT MANAGEMENT | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2 | ACCOUNT MANAGEMENT | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-2 | ACCOUNT MANAGEMENT | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2 | ACCOUNT MANAGEMENT | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC-2 | ACCOUNT MANAGEMENT | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | ACCOUNT MANAGEMENT | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | ACCESS ENFORCEMENT | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| AC-3 | ACCESS ENFORCEMENT | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | ACCESS ENFORCEMENT | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC-3 | ACCESS ENFORCEMENT | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| AC-3 | ACCESS ENFORCEMENT | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| AC-3 | ACCESS ENFORCEMENT | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC-3 | ACCESS ENFORCEMENT | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-3 | ACCESS ENFORCEMENT | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | ACCESS ENFORCEMENT | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-3 | ACCESS ENFORCEMENT | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-3 | ACCESS ENFORCEMENT | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | ACCESS ENFORCEMENT | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | ACCESS ENFORCEMENT | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-3 | ACCESS ENFORCEMENT | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-3 | ACCESS ENFORCEMENT | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | ACCESS ENFORCEMENT | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AC-17 | REMOTE ACCESS | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| AC-17 | REMOTE ACCESS | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-17 | REMOTE ACCESS | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17 | REMOTE ACCESS | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-17 | REMOTE ACCESS | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-17 | REMOTE ACCESS | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| AC-17 | REMOTE ACCESS | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17 | REMOTE ACCESS | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-17 | REMOTE ACCESS | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-17 | REMOTE ACCESS | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-17 | REMOTE ACCESS | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17 | REMOTE ACCESS | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-2 | AUDIT EVENTS | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-2 | AUDIT EVENTS | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-2 | AUDIT EVENTS | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | AUDIT EVENTS | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-3 | CONTENT OF AUDIT RECORDS | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-3 | CONTENT OF AUDIT RECORDS | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-3 | CONTENT OF AUDIT RECORDS | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-3 | CONTENT OF AUDIT RECORDS | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | CONTENT OF AUDIT RECORDS | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-9 | PROTECTION OF AUDIT INFORMATION | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | PROTECTION OF AUDIT INFORMATION | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| AU-9 | PROTECTION OF AUDIT INFORMATION | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | PROTECTION OF AUDIT INFORMATION | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| AU-9 | PROTECTION OF AUDIT INFORMATION | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-11 | AUDIT RECORD RETENTION | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| AU-12 | AUDIT GENERATION | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | AUDIT GENERATION | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | AUDIT GENERATION | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | AUDIT GENERATION | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-12 | AUDIT GENERATION | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | AUDIT GENERATION | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-12 | AUDIT GENERATION | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-12 | AUDIT GENERATION | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-12 | AUDIT GENERATION | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | AUDIT GENERATION | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | AUDIT GENERATION | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | AUDIT GENERATION | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| CA-7 | CONTINUOUS MONITORING | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CA-7 | CONTINUOUS MONITORING | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| CA-7 | CONTINUOUS MONITORING | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | CONTINUOUS MONITORING | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| CM-2 | BASELINE CONFIGURATION | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| CM-2 | BASELINE CONFIGURATION | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CM-2 | BASELINE CONFIGURATION | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CM-2 | BASELINE CONFIGURATION | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| CM-2 | BASELINE CONFIGURATION | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CM-2 | BASELINE CONFIGURATION | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CM-2 | BASELINE CONFIGURATION | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CM-2 | BASELINE CONFIGURATION | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CM-2 | BASELINE CONFIGURATION | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | BASELINE CONFIGURATION | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CM-2 | BASELINE CONFIGURATION | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-7 | LEAST FUNCTIONALITY | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| CM-7 | LEAST FUNCTIONALITY | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-7 | LEAST FUNCTIONALITY | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8 | INFORMATION SYSTEM COMPONENT INVENTORY | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8 | INFORMATION SYSTEM COMPONENT INVENTORY | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8 | INFORMATION SYSTEM COMPONENT INVENTORY | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CM-8 | INFORMATION SYSTEM COMPONENT INVENTORY | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CP-9 | INFORMATION SYSTEM BACKUP | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | INFORMATION SYSTEM BACKUP | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-9 | INFORMATION SYSTEM BACKUP | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | INFORMATION SYSTEM RECOVERY AND RECON STITUTION | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA-5 | AUTHENTICATOR MANAGEMENT | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-5 | AUTHENTICATOR MANAGEMENT | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4 | INCIDENT HANDLING | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4 | INCIDENT HANDLING | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4 | INCIDENT HANDLING | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4 | INCIDENT HANDLING | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4 | INCIDENT HANDLING | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6 | INCIDENT REPORTING | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6 | INCIDENT REPORTING | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6 | INCIDENT REPORTING | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7 | INCIDENT RESPONSE ASSISTANCE | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7 | INCIDENT RESPONSE ASSISTANCE | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7 | INCIDENT RESPONSE ASSISTANCE | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | VULNERABILITY SCANNING | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | VULNERABILITY SCANNING | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | VULNERABILITY SCANNING | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SA-3 | SYSTEM DEVELOPMENT LIFE CYCLE | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3 | SYSTEM DEVELOPMENT LIFE CYCLE | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3 | SYSTEM DEVELOPMENT LIFE CYCLE | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | DENIAL OF SERVICE PROTECTION | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| SC-5 | DENIAL OF SERVICE PROTECTION | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | DENIAL OF SERVICE PROTECTION | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | DENIAL OF SERVICE PROTECTION | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| SC-5 | DENIAL OF SERVICE PROTECTION | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | DENIAL OF SERVICE PROTECTION | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | DENIAL OF SERVICE PROTECTION | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| SC-5 | DENIAL OF SERVICE PROTECTION | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | DENIAL OF SERVICE PROTECTION | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | DENIAL OF SERVICE PROTECTION | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-5 | DENIAL OF SERVICE PROTECTION | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| SC-5 | DENIAL OF SERVICE PROTECTION | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-5 | DENIAL OF SERVICE PROTECTION | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7 | BOUNDARY PROTECTION | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| SC-7 | BOUNDARY PROTECTION | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-7 | BOUNDARY PROTECTION | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-7 | BOUNDARY PROTECTION | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7 | BOUNDARY PROTECTION | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| SC-7 | BOUNDARY PROTECTION | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7 | BOUNDARY PROTECTION | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-7 | BOUNDARY PROTECTION | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | BOUNDARY PROTECTION | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collectio n of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| SC-12 | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12 | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| SC-12 | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | CRYPTOGRAPHIC PROTECTION | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| SC-13 | CRYPTOGRAPHIC PROTECTION | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | CRYPTOGRAPHIC PROTECTION | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-13 | CRYPTOGRAPHIC PROTECTION | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | CRYPTOGRAPHIC PROTECTION | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| SC-13 | CRYPTOGRAPHIC PROTECTION | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | FLAW REMEDIATION | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | FLAW REMEDIATION | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | FLAW REMEDIATION | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SI-2 | FLAW REMEDIATION | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3 | FLAW REMEDIATION | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| SI-3 | FLAW REMEDIATION | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3 | FLAW REMEDIATION | ecs-task-definition-memory-hard-limit | Limiting the maximum memory available to your Amazon Elastic Container Service (ECS) containers ensures that your resource usage cannot be abused in the event of malicious access to your containers. |
| SI-4 | INFORMATION SYSTEM MONITORING | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORING | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORING | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORING | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORIN G | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORIN G | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| SI-4 | INFORMATION SYSTEM MONITORIN G | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORING | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| SI-4 | INFORMATION SYSTEM MONITORING | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORING | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORING | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| SI-4 | INFORMATION SYSTEM MONITORING | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | INFORMATION SYSTEM MONITORING | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| SI-12 | INFORMATION HANDLING AND RETENTION | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| SI-12 | INFORMATION HANDLING AND RETENTION | dynamodb-pitr-enabled | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | INFORMATION HANDLING AND RETENTION | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| SI-16 | MEMORY PROTECTIO N | ecs-task-definition-memory-hard-limit | Limiting the maximum memory available to your Amazon Elastic Container Service (ECS) containers ensures that your resource usage cannot be abused in the event of malicious access to your containers. |

### Template

The template is available on GitHub: Operational Best Practices for FedRAMP(Low).

## Operational Best Practices for FedRAMP(Moderate)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Risk and Authorization Management Program (FedRAMP) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FedRAMP controls. A FedRAMP control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the FedRAMP controls.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(3) | The information system automatic ally disables inactive accounts after 90 days for users. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(3) | The information system automatic ally disables inactive accounts after 90 days for users. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(7) | The organization: (a) Establishes and administers privileged users in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organization: (a) Establishes and administers privileged users in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(7) | The organization: (a) Establishes and administers privileged users in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organization: (a) Establishes and administers privileged users in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organization: (a) Establishes and administers privileged users in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organization: (a) Establishes and administers privileged users in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | account managemen t, network and system administr ation, database administration, and web administration. | | |
| AC-2(12)(a) | The organization: a. Monitors informati on system accounts for [Assignment: organization-defined atypical use]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(12)(a) | The organization: a. Monitors informati on system accounts for [Assignment: organization-defined atypical use]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organizat ion: f. Creates, enables, modifies, disables, and removes information system accounts in accordanc e with [Assignment: organization-defin ed procedures or conditions]. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organizat ion: f. Creates, enables, modifies, disables, and removes information system accounts in accordanc e with [Assignment: organization-defin ed procedures or conditions]. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organizat ion: f. Creates, enables, modifies, disables, and removes information system accounts in accordanc e with [Assignment: organization-defin ed procedures or conditions]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Managemen t (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentia ls. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentia ls. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authoriza tions for logical access to information and system resources in accordance with applicable access control policies. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines information system access authorizations to support separation of duties. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines information system access authorizations to support separation of duties. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC-6(10) | The information system prevents non-privileged users from executing privileged functions to include disabling, circumven ting, or altering implemented security safeguards/counter measures. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(10) | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(10) | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | sagemaker-notebook -no-direct-internet- access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AC-17(1) | The information system monitors and controls remote access methods. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-17(1) | The information system monitors and controls remote access methods. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-17(1) | The information system monitors and controls remote access methods. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-17(1) | The information system monitors and controls remote access methods. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-17(1) | The information system monitors and controls remote access methods. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17(1) | The information system monitors and controls remote access methods. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-17(1) | The information system monitors and controls remote access methods. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implement s cryptographic mechanisms to protect the confident iality and integrity of remote access sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-17(2) | The information system implement s cryptographic mechanisms to protect the confident iality and integrity of remote access sessions. | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-7(1) | The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-7(1) | The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9(2) | The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| AU-9(2) | The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| AU-11 | The organization retains audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored ; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | autoscaling-launch -config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(1) | The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(1) | The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | ebs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | ec2-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | efs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | rds-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-autoscali ng-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/writ e capacity to handle sudden increases in traffic, without throttling. |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | ebs-optimized-inst ance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/ O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contentio n between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| CP-10 | The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-10 | The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(1)(2) | (1) The information system implements multifactor authentic ation for network access to privilege d accounts. (2) The information system implements multifact or authentication for network access to non- privileged accounts. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentia ls. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA-2(1)(2) | (1) The information system implements multifactor authentic ation for network access to privilege d accounts. (2) The information system implements multifact or authentication for network access to non- privileged accounts. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(1)(2) | (1) The information system implements multifactor authentication for network access to privileged accounts. (2) The information system implements multifactor authentication for network access to non- privileged accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1)(2) | (1) The information system implements multifactor authentic ation for network access to privilege d accounts. (2) The information system implements multifact or authentication for network access to non- privileged accounts. | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA-2(1) | (1) The information system implements multifactor authentic ation for network access to privileged accounts. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | (1) The information system implements multifactor authentication for network access to privileged accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | (1) The information system implements multifactor authentication for network access to privileged accounts. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | (1) The information system implements multifactor authentication for network access to privileged accounts. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2 | The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2 | The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(1)(a)(d)(e) | The information system, for password-based authentication: a. Enforces minimum password complexit y of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requireme nts for each type]; d. Enforces password minimum and maximum lifetime restricti ons of [Assignme nt: organization-defined numbers for lifetime minimum, lifetime maximum]; e. Prohibits password reuse for 24 generations | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(4) | The organization employs automated tools to determine if password authentic ators are sufficien tly strong to satisfy [Assignment: organization-defined requirements]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| IA-5(7) | The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6(1) | The organization employs automated mechanisms to assist in the reporting of security incidents. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6(1) | The organization employs automated mechanisms to assist in the reporting of security incidents. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6(1) | The organization employs automated mechanisms to assist in the reporting of security incidents. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7(1) | The organization employs automated mechanisms to increase the availabil ity of incident response-related information and support. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7(1) | The organization employs automated mechanisms to increase the availability of incident response-related information and support. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7(1) | The organization employs automated mechanisms to increase the availabil ity of incident response-related information and support. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5(1) | The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5(1) | The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5(1) | The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | The organization: a. Scans for vulnerabilities in the information system and hosted applications monthly [operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | and results from security control assessments; d. Remediates legitimate vulnerabilities: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery , in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | systemic weaknesses or deficiencies). | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times], in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organizat ion requires the developer of the information system, system component , or information system service to: a. Perform configura tion managemen t during system, component, or service developme nt, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configura tion management]; c. Implement only organization-appro ved changes to the system, component , or service; d. Document approved changes to the system, component , or service and the potential security impacts of such changes; and e. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organizat ion requires the developer of the information system, system component , or information system service to: a. Perform configura tion managemen t during system, component, or service developme nt, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configura tion management]; c. Implement only organization-appro ved changes to the system, component , or service; d. Document approved changes to the system, component , or service and the potential security impacts of such changes; and e. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| SC-4 | The information system prevents unauthorized and unintended information transfer from shared system resources. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended information transfer from shared system resources. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| SC-4 | The information system prevents unauthorized and unintended information transfer from shared system resources. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended information transfer from shared system resources. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-4 | The information system prevents unauthorized and unintended information transfer from shared system resources. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended information transfer from shared system resources. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-4 | The information system prevents unauthorized and unintended information transfer from shared system resources. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | The organization limits the number of external network connections to the information system. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(5) | The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception(i.e., deny all, permit by exception). Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-level-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | sagemaker-notebook -no-direct-internet- access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implement s cryptographic mechanisms to [Selection (one or more): prevent unauthori zed disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implement s cryptographic mechanisms to [Selection (one or more): prevent unauthori zed disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implement s FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | The information system protects the authenticity of communications sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | The information system protects the authenticity of communications sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system component s with regard to flaw remediation. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3 | The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protectio n mechanisms whenever new releases are available in accordance with organizat ional configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the informati on system [Assignme nt: organization-defined frequency ] and real-time scans of files from external sources at [Selection(one or more); endpoint; network entry/exit points] as the files | codebuild-project-envvar-awscred-check | Ensure authentic ation credentials AWS_ACCESS_KEY_ID and AWS_SECRE T_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintende d data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selectio n(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls, electroni c mail servers, web servers, proxy servers, remote-access servers, workstations, | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ns and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | situations, organizat ions rely instead on other safeguard s including, for example, secure coding practices , configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizat ions can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads , and/or actions in response to detection | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. References: NIST Special Publication 800-83. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3 | The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protectio n mechanisms whenever new releases are available in accordance with organizat ional configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the informati on system [Assignme nt: organization-defined frequency ] and real-time scans of files from external sources at [Selection(one or more); endpoint; network entry/exit points] as the files | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selectio n(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls, electroni c mail servers, web servers, proxy servers, remote-access servers, workstations, | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ns and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | situations, organizat ions rely instead on other safeguard s including, for example, secure coding practices , configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizat ions can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads , and/or actions in response to detection | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. References: NIST Special Publication 800-83. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3 | The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protectio n mechanisms whenever new releases are available in accordance with organizat ional configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the informati on system [Assignme nt: organization-defined frequency ] and real-time scans of files from external sources at [Selection(one or more); endpoint; network entry/exit points] as the files | ecs-task-definition-memory-hard-limit | Limiting the maximum memory available to your Amazon Elastic Container Service (ECS) containers ensures that your resource usage cannot be abused in the event of malicious access to your containers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selectio n(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls, electroni c mail servers, web servers, proxy servers, remote-access servers, workstations, | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ns and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | situations, organizat ions rely instead on other safeguard s including, for example, secure coding practices , configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizat ions can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads , and/or actions in response to detection | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. References: NIST Special Publication 800-83. | | |
| SI-4(1) | The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates information from monitoring tools employed throughout the information system. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates information from monitoring tools employed throughout the information system. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| SI-4(16) | The organization correlates information from monitoring tools employed throughout the information system. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates information from monitoring tools employed throughout the information system. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives informati on system security alerts, advisorie s, and directives from [Assignment: organization-defin ed external organizat ions] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignme nt: organization-defined personnel or roles]; [Assignme nt: organization-defined elements within the organizat ion]; [Assignme nt: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives informati on system security alerts, advisorie s, and directives from [Assignment: organization-defin ed external organizat ions] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignme nt: organization-defined personnel or roles]; [Assignme nt: organization-defined elements within the organizat ion]; [Assignme nt: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check security relevant events at least monthly. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check security relevant events at least monthly. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check security relevant events at least monthly. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7 | The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information]. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-16 | The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution. Supplemental Guidance: Some adversaries launch attacks with the intent of executing code in non- executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism. | ecs-task-definition-memory-hard-limit | Limiting the maximum memory available to your Amazon Elastic Container Service (ECS) containers ensures that your resource usage cannot be abused in the event of malicious access to your containers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | Related controls: AC-25, SC-3. Control Enhancements: None. References: None. | | |

### Template

The template is available on GitHub: Operational Best Practices for FedRAMP(Moderate).

## Operational Best Practices for FedRAMP (High Part 1)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Risk and Authorization Management Program (FedRAMP) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FedRAMP controls. A FedRAMP control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17(1) | The information system monitors and controls remote access methods. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| AC-17(1) | The information system monitors and controls remote access methods. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-17(1) | The information system monitors and controls remote access methods. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-17(1) | The information system monitors and controls remote access methods. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-17(1) | The information system monitors and controls remote access methods. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-17(1) | The information system monitors and controls remote access methods. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implement s cryptographic mechanisms to protect the confident iality and integrity of remote access sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-17(2) | The information system implement s cryptographic mechanisms to protect the confident iality and integrity of remote access sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | elb-acm-certificate-required | POPULATE THIS |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protectio n on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(12)(a) | The organization: a. Monitors informati on system accounts for [Assignment: organization-defined atypical use]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(12)(a) | The organization: a. Monitors informati on system accounts for [Assignment: organization-defined atypical use]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(3) | The information system automatic ally disables inactive accounts after 90 days for user accounts. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(3) | The information system automatic ally disables inactive accounts after 90 days for user accounts. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organizat ion: f. Creates, enables, modifies, disables, and removes information system accounts in accordanc e with [Assignment: organization-defin ed procedures or conditions]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organizat ion: f. Creates, enables, modifies, disables, and removes information system accounts in accordanc e with [Assignment: organization-defin ed procedures or conditions]. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organizat ion: f. Creates, enables, modifies, disables, and removes information system accounts in accordanc e with [Assignment: organization-defin ed procedures or conditions]. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as per organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protectio n on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protectio n on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-5c | The organization: c. Defines information system access authorizations to support separation of duties. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines information system access authorizations to support separation of duties. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines information system access authorizations to support separation of duties. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines information system access authorizations to support separation of duties. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-level-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6(2) | The information system requires the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-6(2) | The information system requires the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6(2) | The information system requires the use of non-privileged accounts when accessing nonsecurity functions limits exposure when operating from within privileged accounts or roles | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-6(9) | The information system logs the execution of privileged functions. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | The information system logs the execution of privileged functions. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | The information system logs the execution of privileged functions. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | The information system logs the execution of privileged functions. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AC-6(9) | The information system logs the execution of privileged functions. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | The information system logs the execution of privileged functions. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | The information system logs the execution of privileged functions. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | The information system logs the execution of privileged functions. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(10) | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(10) | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-6(10) | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-11 | The organization retains audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| AU-12(a)(c) | The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizat ional processes for investigation and response to suspiciou s activities. (3) The organization analyzes and correlates audit records across different repositor ies to gain organizat ion-wide situational awareness. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| AU-6(3) | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-6(3) | The organizat ion analyzes and correlates audit records across different repositor ies to gain organizat ion-wide situational awareness. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-6(3) | The organizat ion analyzes and correlates audit records across different repositor ies to gain organizat ion-wide situational awareness. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-6(3) | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-6(3) | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | The organizat ion analyzes and correlates audit records across different repositor ies to gain organizat ion-wide situational awareness. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | The organizat ion analyzes and correlates audit records across different repositor ies to gain organizat ion-wide situational awareness. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | The organizat ion analyzes and correlates audit records across different repositor ies to gain organizat ion-wide situational awareness. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-7 | The information system provides and implements an audit record reduction and report generatio n capability that: a. Supports on-demand audit record review, analysis, and reporting requireme nts and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-7 | The information system provides and implements an audit record reduction and report generatio n capability that: a. Supports on-demand audit record review, analysis, and reporting requireme nts and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-7(1) | The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-7(1) | The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-9(2) | The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| AU-9(2) | The information system backs up audit records at least weekly onto a physically different system or system component than the system or component being audited. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The information system provides audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| CM-2 | The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(1) | The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(1) | The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the presence of unauthorized hardware, software, and firmware components within the information system | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB per node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-6 (1) | The organization identifies an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB per node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | ebs-optimized-inst ance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contentio n between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | redshift-cluster-m aintenancesettings-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | objectives]; andd. Protect the confident iality, integrity, and availability of backup information. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | The information system a. Conduct backups of user-level informati on contained in [Assignment: organization-defined system component s] [Assignment: organization-defined frequency consisten t with recovery time and recovery point objective s];b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives];c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion [Assignment: organization-defined frequency consisten t with recovery time and recovery point | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | objectives]; andd. Protect the confidentiality, integrity, and availability of backup information. | | |
| CP-10 | The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | elb-deletion-prote ction-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | ebs-optimized-inst ance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/ O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contentio n between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB per node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | ec2-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | ebs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | efs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | rds-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB per node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | ec2-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system (daily incremental; weekly full). | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2 | The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2 | The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | (1) The information system implements multifactor authentication for network access to privileged accounts. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(1) | (1) The information system implements multifactor authentication for network access to privileged accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(1)(2) | (1) The information system implements multifactor authentic ation for network access to privilege d accounts. (2) The information system implements multifact or authentication for network access to non- privileged accounts. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protectio n on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(1)(2) | (1) The information system implements multifactor authentic ation for network access to privilege d accounts. (2) The information system implements multifact or authentication for network access to non- privileged accounts. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protectio n on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-5(1)(a)(d)(e) | The information system, for password-based authentication: a. Enforces minimum password complexit y of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requireme nts for each type]; d. Enforces password minimum and maximum lifetime restricti ons of [Assignme nt: organization-defined numbers for lifetime minimum, lifetime maximum]; e. Prohibits password reuse for 24 generations | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(4) | The organization employs automated tools to determine if password authentic ators are sufficien tly strong to satisfy [Assignment: organization-defined requirements]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| IA-5(7) | The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6(1) | The organization employs automated mechanisms to assist in the reporting of security incidents. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6(1) | The organization employs automated mechanisms to assist in the reporting of security incidents. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6(1) | The organization employs automated mechanisms to assist in the reporting of security incidents. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7(1) | The organization employs automated mechanisms to increase the availability of incident response-related information and support. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7(1) | The organization employs automated mechanisms to increase the availabil ity of incident response-related information and support. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7(1) | The organization employs automated mechanisms to increase the availabil ity of incident response-related information and support. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times], in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| RA-5 | The organization: a. Scans for vulnerabilities in the information system and hosted applications monthly [operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | and results from security control assessments; d. Remediates legitimate vulnerabilities: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery , in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | systemic weaknesses or deficiencies). | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organizat ion requires the developer of the information system, system component , or information system service to: a. Perform configura tion managemen t during system, component, or service developme nt, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configura tion management]; c. Implement only organization-appro ved changes to the system, component , or service; d. Document approved changes to the system, component , or service and the potential security impacts of such changes; and e. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organizat ion requires the developer of the information system, system component , or information system service to: a. Perform configura tion managemen t during system, component, or service developme nt, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configura tion management]; c. Implement only organization-appro ved changes to the system, component , or service; d. Document approved changes to the system, component , or service and the potential security impacts of such changes; and e. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, AND operation; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authorization for accessing GitHub or Bitbucket repositories. |
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | The information system protects the authenticity of communications sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | The information system protects the authenticity of communications sessions. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | The information system protects the authenticity of communications sessions. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the confidentiality AND integrity of [Assignment: organization-defined information at rest]. | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended information transfer via shared system resources. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| SC-4 | The information system prevents unauthorized and unintended information transfer via shared system resources. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended information transfer via shared system resources. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC-4 | The information system prevents unauthorized and unintended information transfer via shared system resources. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer via shared system resources. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | sagemaker-notebook -no-direct-internet- access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-level-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | The organization limits the number of external network connections to the information system. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | The organization limits the number of external network connections to the information system. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the confidentiality AND integrity of transmitted information. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-8(1) | The information system implement s cryptographic mechanisms to [Selection (one or more): prevent unauthori zed disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implement s cryptographic mechanisms to [Selection (one or more): prevent unauthori zed disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB per node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system component s with regard to flaw remediation. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms at least monthly to determine the state of information system component s with regard to flaw remediation. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environme nt ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| SI-4(1) | The organizat ion connects and configures individua l intrusion detection tools into an information system-wide intrusion detection system. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates information from monitoring tools employed throughout the information system. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates information from monitoring tools employed throughout the information system. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-4(5) | The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization- defined compromise indicators]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7 | The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information]. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check security relevant events at least monthly. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check security relevant events at least monthly. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check security relevant events at least monthly. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5(1) | The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Suppleme ntal Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabi lities are discovere d, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5(1) | The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5(1) | The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(5) | The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception(i.e., deny all, permit by exception). Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(7) | The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | key management, account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | key management, account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | key management, account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one IAM user. Placing IAM users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | key management, account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(7) | The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | key management, account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(7) | The organizat ion: (a) Establish es and administe rs privileged user accounts in accordanc e with a role-based access scheme that organizes allowed information system access and privilege s into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignme nt: organization-defined actions] when privileged role assignmen ts are no longer appropriate. Supp lemental Guidance: Privileged roles are organization-defin ed roles assigned to individuals that allow those individua ls to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | key management, account managemen t, network and system administr ation, database administration, and web administration. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-11 | The information system: a. Generates error messages that provide informati on necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defin ed personnel or roles]. Supplemental Guidance: Organizat ions carefully consider the structure /content of error messages. The extent to which informati on systems are able to identify and handle error conditions is guided by organizational policy and operation al requirements. Information that could be exploited by adversaries includes, for example, erroneous logon | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | attempts with passwords entered by mistake as the username, mission/business informati on that can be derived from(if not stated explicitl y by) informati on recorded, and personal informati on such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitt ing information. Related controls: AU-2, AU-3, SC-31. C ontrol Enhancements: None. References: None. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3 | The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protectio n mechanisms whenever new releases are available in accordance with organizat ional configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the informati on system [Assignme nt: organization-defined frequency ] and real-time scans of files from external sources at [Selection(one or more); endpoint; network entry/exit points] as the files | codebuild-project-envvar-awscred-check | Ensure authentic ation credentials AWS_ACCESS_KEY_ID and AWS_SECRE T_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintende d data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selectio n(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls, electroni c mail servers, web servers, proxy servers, remote-access servers, workstations, | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(e .g., UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ns and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | situations, organizat ions rely instead on other safeguard s including, for example, secure coding practices , configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizat ions can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads , and/or actions in response to detection | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. References: NIST Special Publication 800-83. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3 | The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protectio n mechanisms whenever new releases are available in accordance with organizat ional configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the informati on system [Assignme nt: organization-defined frequency ] and real-time scans of files from external sources at [Selection(one or more); endpoint; network entry/exit points] as the files | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, user name and password within AWS Codebuild project environments. Use OAuth instead of personal access tokens or a user name and password to grant authoriza tion for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selectio n(one or more): block malicious code; quarantine malicious code; send alert to administr ator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Informati on system entry and exit points include, for example, firewalls, electroni c mail servers, web servers, proxy servers, remote-access servers, workstations, | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(e .g., UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ns and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | situations, organizat ions rely instead on other safeguard s including, for example, secure coding practices , configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizat ions can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads , and/or actions in response to detection | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. References: NIST Special Publication 800-83. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives informati on system security alerts, advisorie s, and directives from [Assignment: organization-defin ed external organizat ions] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignme nt: organization-defined personnel or roles]; [Assignme nt: organization-defined elements within the organizat ion]; [Assignme nt: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives informati on system security alerts, advisorie s, and directives from [Assignment: organization-defin ed external organizat ions] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignme nt: organization-defined personnel or roles]; [Assignme nt: organization-defined elements within the organizat ion]; [Assignme nt: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-5 | The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection(one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | the issuing organizat ion of the degree of noncompliance. Su pplemental Guidance: The United States Computer Emergency Readiness Team(US-CERT) generates security alerts and advisories to maintain situational awareness across the federal governmen t. Security directive s are issued by OMB or other designated organizations with the responsibility and authority to issue such directive s. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects o n organizational operations and assets, individua ls, other organizat ions, and the Nation should the directives not be implemented | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | in a timely manner. External organizat ions include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supp orting organizations. Related control: SI-2. References: NIST Special Publication 800-40. | | |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at all information system and network components where audit capability is deployed/available c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authoriza tion checks, data deletions, data access, data changes, and permissio n changes. d. Determines that the following events are to be audited within the informati on system: [organiza tion-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

### Template

The template is available on GitHub: Operational Best Practices for FedRAMP (High Part 1).

## Operational Best Practices for FedRAMP (High Part 2)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Risk and Authorization Management Program (FedRAMP) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FedRAMP controls. A FedRAMP control can be

related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-02 (11) | The information system enforces organization-defined circumstances and/or usage conditions for organization-defined system accounts. | guardduty-enabled-centralized | Use Amazon GuardDuty to monitor the use of short term credentials associated with IAM instance roles. Amazon GuardDuty is able to check for credential exfiltration in IAM Instance Profiles using UnauthorizedAccess check. |
| AC-02 (12)(a) | The organization: a. Monitors information system accounts for [Assignment: organization-defined atypical use]. | cloudtrail-security-trail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-06 (03) | The organization authorizes network access to assigned personnel only when it is needed to complete the task for access for the security plan. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-06 (03) | The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system. | eks-endpoint-no-public-access | Manage access your to Amazon Elastic Kubernetes Service (Amazon EKS) cluster by ensuring that the Kubernetes API server endpoint is not publicly accessible. By restricting public access to the Kubernetes API server endpoint, you can reduce the risk of unauthorized access to your EKS cluster and its resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-05 (02) | The information system provides a warning to key personnel within the set time when allocated audit log storage volume reaches set percentage of repository maximum audit log storage capacity. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-06 (04) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-06 (05) | The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and system monitoring information to further enhance the ability to identify inappropriate or unusual activity. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (05) | The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning informati on; performan ce data; system monitoring informati on; [Assignment: organization-defin ed data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-06 (07) | The organization specify permitted actions for each system process, role, and user associated with the review, analysis, and reporting of audit record information. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| AU-06 (07) | The organization specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-09 (02) | The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| AU-09 (02) | The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-09 (02) | The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| AU-09 (02) | The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-09 (03) | The information system provides irrefutable evidence that an individual has performed. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| AU-09 (03) | The information system restricts network access to audit log data. | cloudtrail-s3-bucket-public-access-prohibited | Ensures that S3 buckets used to store CloudTrail logs are not publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-10 | The information system provides irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation]. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AU-10 | The information system provides irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation]. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-10 | The information system provides irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation]. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system component s] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defin ed level of tolerance for the relationship between time stamps of individual records in the audit trail]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system component s] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defin ed level of tolerance for the relationship between time stamps of individual records in the audit trail]. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system component s] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defin ed level of tolerance for the relationship between time stamps of individual records in the audit trail]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail]. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail]. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail]. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail]. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system component s] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defin ed level of tolerance for the relationship between time stamps of individual records in the audit trail]. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | The organization compiles audit records from [Assignment: organization-defined system component s] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defin ed level of tolerance for the relationship between time stamps of individual records in the audit trail]. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-03 | The organization determines and documents the types of changes to the system that are configuration-cont rolled. | rds-instance-delet ion-protection-ena bled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-08 (02) | The organization maintains the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms]. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-08 (02) | The organization maintains the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms]. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-08 (02) | The organization maintains the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms]. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-02 (05) | The orgainization provides for the plan for the continuance of mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | backup-recovery-point-minimum-retention-check | Checks if a recovery point expires no earlier than after the specified period. Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | rds-in-backup-plan | Checks if Amazon Relational Database Service (Amazon RDS) databases are present in AWS Backup plans. Organizations establish recovery time and recovery point objectives as part of contingency planning. Configura tion of the alternate storage site includes physical facilitie s and the systems supporting recovery operations that ensure accessibility and correct execution . |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | dynamodb-in-backup -plan | Checks whether Amazon DynamoDB table is present in AWS Backup Plans. Organizations establish recovery time and recovery point objectives as part of contingency planning. Configura tion of the alternate storage site includes physical facilitie s and the systems supporting recovery operations that ensure accessibility and correct execution . |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-06 (02) | The organization configures the alternate storage site to facilitate recovery operation s in accordance with recovery time and recovery point objectives. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-07 (01) | The orgainization identifies an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-07 (04) | The organizat ion prepares the alternate processin g site so that the site can serve as the operational site supporting essential mission and business functions. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-07 (04) | The organizat ion prepares the alternate processin g site so that the site can serve as the operational site supporting essential mission and business functions. | backup-recovery-po int-encrypted | Checks if a recovery point is encrypted . Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considera tions are in place. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-07 (04) | The organizat ion prepares the alternate processin g site so that the site can serve as the operational site supporting essential mission and business functions. | backup-recovery-po int-manual-deletion-disabled | Checks if a backup vault has an attached resource-based policy which prevents deletion of recovery points. Site preparati on includes establish ing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considera tions are in place. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-07 (04) | The organization prepares the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions. | s3-bucket-cross-region-replication-enabled | Checks if you have enabled S3 Cross-Region Replication for your Amazon S3 buckets. Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | backup-recovery-point-minimum-retention-check | Checks if a recovery point expires no earlier than after the specified period. Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may provide separate storage |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | by implementing automated backup processes at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire rated containers. |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | s3-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Simple Storage Service (Amazon S3) buckets are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (03) | The organization store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire rated container that is not collocated with the operational system. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-09 (05) | The organization transfers system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (05) | The organization transfers system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. | backup-recovery-point-minimum-retention-check | Checks if a recovery point expires no earlier than after the specified period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (05) | The organization transfers system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (05) | The organization transfers system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (05) | The organization transfers system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-09 (08) | The organization employs cryptographic mechanisms to prevent unauthorized disclosure backup information. | backup-recovery-point-encrypted | The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 (04) | The organization provides the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components. | backup-recovery-point-encrypted | Enable this rule to check if a recovery point is encrypted. |
| CP-10 (04) | The organization provides the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components. | backup-recovery-point-minimum-retention-check | Enable this rule to chek that if a recovery point expires no ealier than after the specified period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 (04) | The organization provides the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| CP-10 (04) | The organization provides the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 (04) | The organizat ion provides the capability to restore system component s within [Assignme nt: organization-defined restoration time periods] from configuration-cont rolled and integrity-protected informati on representing a known, operation al state for the components. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| IA-02 (02) | Implement multi-fac tor authentication for access to non-privi leged accounts. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-02 (02) | Implement multi-factor authentication for access to non-privileged accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-02 (06) | The information system Implements multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that: (a) One of the factors is provided by a device separate from the system gaining access; and (b) The device meets [Assignment: organization-defined strength of mechanism requirements]. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-02 (06) | The information system Implements multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that: (a) One of the factors is provided by a device separate from the system gaining access; and (b) The device meets [Assignment: organization-defined strength of mechanism requirements]. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-02 (08) | The information system implements replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts]. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-05 (08) | The information system implements [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| IA-05 (08) | The information system implements [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-05 (08) | The information system implements [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-05 (08) | The information system implements [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-05 (08) | The information system implements [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-05 (08) | The information system implements [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring IAM users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-04 (04) | The organization employs automated mechanisms to correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-04 (04) | The organization employs automated mechanisms to correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| IR-04 (04) | The organization employs automated mechanisms to correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-04 (04) | The organization employs automated mechanisms to correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IR-04 (04) | The organization employs automated mechanisms to correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| RA-05 | Monitor and scan for vulnerabilities hosted applications and when new vulnerabi lities potentially affect the system are identified and reported | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-05 | Define the breadth and depth of vulnerability scanning coverage. | inspector-lambda-standard-scan-enabled | Checks if Amazon Inspector V2 Lambda standard scanning is activated for your single or multi-account environment to detect potential software vulnerabilities. The rule is NON_COMPLIANT if Lambda standard scanning is not activated. |
| RA-05 | Define the breadth and depth of vulnerability scanning coverage. | inspector-ec2-scan-enabled | Checks if Amazon Inspector V2 EC2 scanning is activated for your single or multi-account environment to detect potential vulnerabilities and network reachability issues on your EC2 instances. The rule is NON_COMPLIANT if EC2 scanning is not activated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-05 | Define the breadth and depth of vulnerability scanning coverage. | inspector-ecr-scan-enabled | Checks if Amazon Inspector V2 ECR scanning is activated for your single or multi-account environment to detect potential software vulnerabilities in your container images. The rule is NON_COMPLIANT if ECR scanning is not activated. |
| RA-05 (03) | Define the breadth and depth of vulnerability scanning coverage. | inspector-lambda-standard-scan-enabled | Checks if Amazon Inspector V2 Lambda standard scanning is activated for your single or multi-account environment to detect potential software vulnerabilities. The rule is NON_COMPLIANT if Lambda standard scanning is not activated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-05 (03) | Define the breadth and depth of vulnerability scanning coverage. | inspector-ec2-scan-enabled | Checks if Amazon Inspector V2 EC2 scanning is activated for your single or multi-account environment to detect potential vulnerabilities and network reachability issues on your EC2 instances. The rule is NON_COMPLIANT if EC2 scanning is not activated. |
| RA-05 (03) | Define the breadth and depth of vulnerability scanning coverage. | inspector-ecr-scan-enabled | Checks if Amazon Inspector V2 ECR scanning is activated for your single or multi-account environment to detect potential software vulnerabi lities in your container images. The rule is NON_COMPL IANT if ECR scanning is not activated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-05 (05) | Implement privileged access authorization to [Assignment: organization-defined system components] for scannig of organization. (Specifies all components that support authentication and all scans) | inspector-ec2-scan-enabled | Checks if Amazon Inspector V2 EC2 scanning is activated for your single or multi-account environment to detect potential vulnerabilities and network reachability issues on your EC2 instances. The rule is NON_COMPLIANT if EC2 scanning is not activated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The orgainization requires the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |
| SC-07 (12) | The orgainization implements [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components]. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-07 (20) | Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-07 (21) | Employ boundary protection mechanisms to isolate [Assignment: organization-defined system component s] supporting [Assignment: organization-defin ed missions and/or business functions]. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-07(21) | Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions]. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12 (01) | Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| SC-28 (01) | The organization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-28 (01) | The orgainization implements cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information]. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (12) | Alert [Assignment: organization-defined personnel or roles] using [Assignme nt: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activitie s with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts]. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (20) | Implement the following additiona l monitoring of privileged users: [Assignment: organization-defined additional monitorin g]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (20) | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (20) | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (20) | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-04 (20) | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (20) | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| SI-04 (20) | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (20) | Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring]. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (20) | Implement the following additiona l monitoring of privileged users: [Assignment: organization-defined additional monitorin g]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (22) | (a) Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and (b) [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected. | securityhub-enabled | (A) AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-04 (22) | (a) Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and (b) [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| SI-04 (22) | (a) Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and (b) [Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-05 (01) | Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-05 (01) | Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-07 (02) | Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-07 (02) | Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-07 (05) | Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-07 (05) | Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SI-07 (15) | Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components]. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-07 (15) | Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components]. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

### Template

The template is available on GitHub: Operational Best Practices for FedRAMP (High Part 2).

## Operational Best Practices for FFIEC

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Federal Financial Institutions Examination Council (FFIEC) Cyber Security Assessment Tool domains and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more FFIEC Cyber Security Assessment Tool controls. A FFIEC Cyber Security Assessment Tool control can be related to

multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.G.IT.B.1 | An inventory of organizational assets (for example, hardware, software, data, and systems hosted externally) is maintained. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| D1.G.IT.B.1 | An inventory of organizational assets (for example, hardware, software, data, and systems hosted externally) is maintained. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| D1.G.IT.B.1 | An inventory of organizational assets (for example, hardware, software, data, and systems hosted externally) is maintained. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.G.IT.B.1 | An inventory of organizational assets (for example, hardware, software, data, and systems hosted externally) is maintained. | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.Rm.B.1 | An information security and business continuity risk management function(s) exists within the institution. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| D1.RM.RA.B.2 | The risk assessment identifies Internet-based systems and high-risk transactions that warrant additional authentication controls. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D1.RM.RA.B.2 | The risk assessment identifies Internet-based systems and high-risk transactions that warrant additional authentication controls. | annual-risk-assessment-performed (process check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting an organization. |
| D1.TC.Tr.B.2 | Annual information security training includes incident response, current cyber threats (for example,phishing, spear phishing, social engineering, and mobile security), and emerging issues. | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.IS.Is.B.1 | Information security threats are gathered and shared with applicable internal employees. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| D2.IS.Is.B.1 | Information security threats are gathered and shared with applicable internal employees. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.IS.Is.B.1 | Information security threats are gathered and shared with applicable internal employees. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| D2.MA.Ma.B.1 | Audit log records and other security event logs are reviewed and retained in a secure manner. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.MA.Ma.B.2 | Computer event logs are used for investigations after an event has occurred. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.TI.Ti.B.1 | The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (for example, FS-ISAC, US- CERT). | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.TI.Ti.B.1 | The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (for example, FS-ISAC, US- CERT). | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| D2.TI.Ti.B.2 | Threat information is used to monitor threats and vulnerabilities. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.TI.Ti.B.2 | Threat information is used to monitor threats and vulnerabi lities. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.TI.Ti.B.2 | Threat information is used to monitor threats and vulnerabilities. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.TI.Ti.B.3 | Threat informati on is used to enhance internal risk management and controls. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D2.TI.Ti.B.3 | Threat informati on is used to enhance internal risk management and controls. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| D3.CC.PM.B.1 | A patch managemen t program is implemented and ensures that software and firmware patches are applied in a timely manner. | ec2-managedinstanc e-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.CC.PM.B.1 | A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| D3.CC.PM.B.1 | A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.CC.PM.B.1 | A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.CC.PM.B.3 | Patch management reports are reviewed and reflect missing security patches. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| D3.CC.PM.B.3 | Patch management reports are reviewed and reflect missing security patches. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.CC.PM.B.3 | Patch management reports are reviewed and reflect missing security patches. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.CC.PM.B.3 | Patch management reports are reviewed and reflect missing security patches. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.1 | The institution is able to detect anomalous activities through monitoring across the environment. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.DC.An.B.1 | The institution is able to detect anomalous activities through monitoring across the environment. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.DC.An.B.1 | The institution is able to detect anomalous activities through monitoring across the environment. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| D3.DC.An.B.2 | Customer transacti ons generating anomalous activity alerts are monitored and reviewed. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.2 | Customer transactions generating anomalous activity alerts are monitored and reviewed. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.3 | Logs of physical and/or logical access are reviewed following events. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| D3.DC.An.B.4 | Access to critical systems by third parties is monitored for unauthorized or unusual activity | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.An.B.5 | Elevated privileges are monitored. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| D3.DC.An.B.5 | Elevated privileges are monitored. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Ev.B.1 | A normal network activity baseline is established. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| D3.DC.Ev.B.2 | Mechanisms (for example, antivirus alerts, log event alerts) are in place to alert management to potential attacks. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Ev.B.3 | Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| D3.DC.Ev.B.3 | Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.DC.Ev.B.3 | Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.DC.Ev.B.3 | Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| D3.DC.Th.B.1 | Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Th.B.1 | Independent testing (including penetration testing and vulnerabi lity scanning) is conducted according to the risk assessmen t for external-facing systems and the internal network. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.DC.Th.B.1 | Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.1 | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.10 | Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no productio n environment exists at the institution or the institution's third-party.) | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.10 | Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no productio n environment exists at the institution or the institution's third-party.) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.10 | Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no productio n environment exists at the institution or the institution's third-party.) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.10 | Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no productio n environment exists at the institution or the institution's third-party.) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.12 | All passwords are encrypted in storage and in transit. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| D3.PC.Am.B.13 | Confidential data is encrypted when transmitted across public or untrusted networks (for example, Internet). | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.13 | Confidential data is encrypted when transmitted across public or untrusted networks (for example, Internet). | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| D3.PC.Am.B.13 | Confidential data is encrypted when transmitted across public or untrusted networks (for example, Internet). | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.13 | Confidential data is encrypted when transmitted across public or untrusted networks (for example, Internet). | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| D3.PC.Am.B.13 | Confidential data is encrypted when transmitted across public or untrusted networks (for example, Internet). | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| D3.PC.Am.B.13 | Confidential data is encrypted when transmitted across public or untrusted networks (for example, Internet). | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.13 | Confidential data is encrypted when transmitted across public or untrusted networks (for example, Internet). | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| D3.PC.Am.B.15 | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.15 | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.15 | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.15 | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.15 | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| D3.PC.Am.B.15 | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| D3.PC.Am.B.15 | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.16 | Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.16 | Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |
| D3.PC.Am.B.16 | Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.16 | Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| D3.PC.Am.B.2 | Employee access to systems and confidential data provides for separation of duties. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.2 | Employee access to systems and confidential data provides for separation of duties. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| D3.PC.Am.B.2 | Employee access to systems and confidential data provides for separation of duties. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.3 | Elevated privileges (for example, administrator privileges) are limited and tightly controlled (for example, assigned to individuals, not shared, and require stronger password controls) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.3 | Elevated privileges (for example, administrator privileges) are limited and tightly controlled (for example, assigned to individuals, not shared, and require stronger password controls) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.3 | Elevated privileges (for example, administrator privileges) are limited and tightly controlled (for example, assigned to individuals, not shared, and require stronger password controls). | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.3 | Elevated privileges (for example, administrator privileges) are limited and tightly controlled (for example, assigned to individuals, not shared, and require stronger password controls) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.3 | Elevated privileges (for example, administrator privileges) are limited and tightly controlled (for example, assigned to individuals, not shared, and require stronger password controls) | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| D3.PC.Am.B.3 | Elevated privileges (for example, administrator privileges) are limited and tightly controlled (for example, assigned to individuals, not shared, and require stronger password controls) | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applicati ons, and hardware. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applicati ons, and hardware. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| D3.PC.Am.B.6 | Identification and authentication are required and managed for access to systems, applications, and hardware. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.7 | Access controls include password complexity and limits to password attempts and reuse. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Am.B.8 | All default passwords and unnecessary default accounts are changed before system implement ation. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| D3.PC.Im.B.1 | Network perimeter defense tools (for example, border router and firewall) are used. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.2 | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.2 | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.2 | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.IM.B.2 | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.2 | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| D3.PC.IM.B.2 | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.3 | All ports are monitored. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| D3.PC.IM.B.3 | All ports are monitored. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.3 | All ports are monitored. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| D3.PC.IM.B.3 | All ports are monitored. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.3 | All ports are monitored. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.3 | All ports are monitored. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.5 | Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.5 | Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.5 | Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.6 | Ports, functions , protocols and services are prohibite d if no longer needed for business purposes. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.6 | Ports, functions , protocols and services are prohibite d if no longer needed for business purposes. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.6 | Ports, functions , protocols and services are prohibite d if no longer needed for business purposes. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.IM.B.6 | Ports, functions , protocols and services are prohibite d if no longer needed for business purposes. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.7 | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| D3.PC.Im.B.7 | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D3.PC.Im.B.7 | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.7 | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.7 | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| D3.PC.Im.B.7 | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Im.B.7 | Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| D3.PC.Se.B.1 | Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D3.PC.Se.B.1 | Developers working for the instituti on follow secure program coding practices, as part of a system developme nt life cycle (SDLC), that meet industry standards. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D4.C.Co.B.2 | The institution ensures that third-party connections are authorized. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D4.C.Co.B.2 | The institution ensures that third-party connections are authorized. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D4.C.Co.B.2 | The institution ensures that third-party connections are authorized. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D4.C.Co.B.2 | The institution ensures that third-party connections are authorized. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.1 | Alert parameters are set for detecting information security incidents that prompt mitigating actions. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.1 | Alert parameters are set for detecting information security incidents that prompt mitigating actions. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.1 | Alert parameters are set for detecting information security incidents that prompt mitigating actions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| D5.DR.De.B.2 | System performan ce reports contain information that can be used as a risk indicator to detect information security incidents | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.2 | System performance reports contain information that can be used as a risk indicator to detect information security incidents | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.DR.De.B.3 | Tools and processes are in place to detect, alert, and trigger the incident response program. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.ER.Es.B.4 | Incidents are classified, logged and tracked. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |
| D5.IR.Pl.B.1 | The institution has documented how it will react and respond to cyber incidents. | response-plan-exists-maintained (process check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | lambda-concurrency-check | This rule ensures that a Lambda function' s concurrency high and low limits are established. This can assist in baselinin g the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| D5.IR.Pl.B.6 | The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

### Template

The template is available on GitHub: Operational Best Practices for FFIEC.

## Operational Best Practices for Germany Cloud Computing Compliance Criteria Catalog (C5)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Germany Cloud Computing Compliance Criteria Catalog (C5) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more Germany C5 controls. A Germany C5 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-01 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| COS-01 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| COS-01 | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no conditions could result in unintended behavior. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-01 | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |
| COS-01 | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collection of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| COS-01 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| COS-03 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| COS-03 | ebs-snapshot-public-restora ble-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| COS-03 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| COS-03 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| COS-03 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| COS-03 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| COS-03 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| COS-03 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |
| COS-03 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| COS-03 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| COS-03 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-03 | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configure d to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| COS-05 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| COS-05 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-05 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| COS-05 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| COS-05 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-05 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| COS-05 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| COS-05 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-05 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| COS-05 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-05 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| COS-05 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| COS-05 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| CRY-02 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CRY-02 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-02 | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |
| CRY-02 | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-02 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CRY-02 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CRY-02 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-02 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CRY-02 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CRY-03 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-03 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| CRY-03 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| CRY-03 | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| CRY-03 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-03 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| CRY-03 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| CRY-03 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-03 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CRY-03 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| CRY-03 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| CRY-03 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| CRY-03 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-03 | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| CRY-03 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| CRY-03 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-03 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| CRY-03 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| CRY-03 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-03 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| CRY-04 | cmk-backing-key-rotation-en abled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |
| DEV-07 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| DEV-07 | codebuild-project-logging-e nabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| DEV-07 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| DEV-07 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| DEV-07 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| DEV-07 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
|---|---|---|
| | | actual values should reflect your organization's policies. |
| IDM-01 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| IDM-01 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authoriza tions, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| IDM-01 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| IDM-01 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IDM-01 | secretsmanager-rotation-ena bled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |
| IDM-01 | secretsmanager-scheduled-ro tation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potential ly reduce the business impact if it is compromised. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |
| IDM-01 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| IDM-01 | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |
| IDM-01 | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| IDM-01 | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |
| IDM-01 | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| IDM-01 | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-01 | rds-instance-iam-authentication-enabled | Ensure an AWS Identity and Access Managemen t (IAM) authentication is enabled on Amazon Relationa l Database Service (Amazon RDS) instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). You are not required to store user credentials in the database, as authentication is managed externally. |
| IDM-01 | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-03 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| IDM-03 | secretsmanager-secret-unuse d | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organizat ion's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-08 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| CRY-01 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
|---|---|---|
| | | actual values should reflect your organization's policies. |
| IDM-09 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| IDM-09 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| IDM-09 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IDM-09 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-01 | clb-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availabil ity zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |
| OPS-01 | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availabil ity zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |
| OPS-01 | lambda-vpc-multi-az-check | If your AWS Lambda function is configured to connect to a virtual private cloud (VPC) in your account, deploy the AWS Lambda function in at least two different Availabil ity Zones to ensure that it is your function is available to process events in case of a service interruption in a single zone. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-01 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-01 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-01 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| OPS-01 | elb-cross-zone-load-balanci ng-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zon e load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your applicati on's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-01 | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughpu t capacity is checked on your Amazon DynamoDB tables. This is the amount of read/ write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approache s the maximum limit for a customer's account. This rule allows you to optionall y set accountRCUThreshol dPercentage (Config Default: 80) and accountWCUThreshol dPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |
| OPS-02 | clb-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availabil ity zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-02 | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |
| OPS-02 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-02 | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availabil ity zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |
| OPS-02 | lambda-vpc-multi-az-check | If your AWS Lambda function is configured to connect to a virtual private cloud (VPC) in your account, deploy the AWS Lambda function in at least two different Availabil ity Zones to ensure that it is your function is available to process events in case of a service interruption in a single zone. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-02 | rds-cluster-multi-az-enabled | Amazon Relational Database Service (Amazon RDS) clusters should have Multi-AZ replication enabled to assist in the availability of the data that is stored. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-02 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-02 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| OPS-02 | elb-cross-zone-load-balanci ng-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zon e load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your applicati on's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-02 | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughpu t capacity is checked on your Amazon DynamoDB tables. This is the amount of read/ write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approache s the maximum limit for a customer's account. This rule allows you to optionall y set accountRCUThreshol dPercentage (Config Default: 80) and accountWCUThreshol dPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |
| OPS-07 | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| OPS-07 | opensearch-data-node-fault-tolerance | Amazon OpenSearch Service (OpenSearch Service) requires at least three data nodes for high availability and fault-tolerance. Deploying an OpenSearch Service domain with at least three data nodes ensures cluster operations if a node fails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |
| OPS-07 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| OPS-07 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |
| OPS-07 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| OPS-07 | fsx-resources-protected-by-backup-plan | To help with data backup processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-07 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |
| OPS-07 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-12 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| OPS-12 | s3-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| OPS-13 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-13 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-13 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| OPS-14 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-14 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| OPS-14 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| OPS-14 | s3-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| OPS-15 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-15 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| OPS-15 | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |
| OPS-15 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-15 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| OPS-15 | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| OPS-15 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-15 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| OPS-15 | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| OPS-15 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-15 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| OPS-15 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-15 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| OPS-15 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| OPS-15 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| OPS-15 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| OPS-22 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| PSS-05 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| PSS-05 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| PSS-05 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| PSS-05 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| PSS-07 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |

### Template

The template is available on GitHub: Germany Cloud Computing Compliance Criteria Catalog (C5).

## Operational Best Practices for Gramm Leach Bliley Act (GLBA)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Gramm-Leach-Bliley Act (GLBA) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more GLBA controls. A GLBA control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | technical, and physical safeguards | | |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | internet-gateway-a uthorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | sagemaker-notebook -no-direct-internet- access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | autoscaling-launch -config-public-ip- disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | s3-bucket-level-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | api-gw-cache-enabl ed-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | cloudwatch-log-gro up-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | elasticsearch-encr ypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | rds-storage-encryp ted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | s3-bucket-server-s ide-encryption-ena bled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | sagemaker-endpoint -configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | sagemaker-notebook -instance-kms-key- configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | dynamodb-table-enc rypted-kms | Ensure that encryptio n is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | rds-snapshot-encry pted | Ensure that encryptio n is enabled for your Amazon Relationa l Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | opensearch-encrypt ed-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | opensearch-node-to -node-encryption-c heck | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(1) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguard s (1) to insure the security and confidentiality of customer records and information; | kinesis-stream-enc rypted | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(2) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(2) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | secretsmanager-rot ation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | s3-bucket-policy-g rantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_gran tee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principal s, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Managemen t (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentia ls. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | opensearch-access-control-enabled | Ensure fine-grai ned access control is enabled on your Amazon OpenSearc h Service domains. Fine-grained access control provides enhanced authoriza tion mechanisms to achieve least-pri vileged access to Amazon OpenSearc h Service domains. It allows for role-base d access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-ten ancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | ecs-containers-rea donly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance' s filesystem cannot be modified unless it has explicit read-writ e permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | efs-access-point-e nforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirect ory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| GLBA-SEC.501(b)(3) | In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropria te standards for the financial instituti ons subject to their jurisdiction relating to administrative, technical, and physical safeguards (3) to protect against unauthorized access to or use of such records or informati on which could result in substantial harm or inconvenience to any customer. | efs-access-point-e nforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configure d on the access point for all file system operations and only grants access to this enforced user identity. |

### Template

The template is available on GitHub: Operational Best Practices for Gramm Leach Bliley Act (GLBA).

## Operational Best Practices for GxP EU Annex 11

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the GxP EU Annex 11 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more GxP EU Annex 11 controls. A GxP EU Annex 11 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1. Risk Management | Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk managemen t system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 1. Risk Management | Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk managemen | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | t system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system. | | or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 4.2. Validation - Documentation Change Control | Validation documentation should include change control records (if applicabl e) and reports on any deviations observed during the validation process. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3. Validation - Inventory | An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3. Validation - Inventory | An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3. Validation - Inventory | An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. | ec2-security-group-attached-to-eni-periodic | To help manage your asset inventory, this rule checks if security groups are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or to an elastic network interface. If your security groups are not attached to these resource types, they may be unused and no longer needed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3. Validation - Inventory | An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3. Validation - Inventory | An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangeme nts, data flows and interfaces with other systems or processes , any hardware and software pre-requi sites, and security measures should be available. | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.3. Validation - Inventory | An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 4.8. Validation - Data Transfer | If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchangin g data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchangin g data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 5. Data | Computerised systems exchangin g data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchangin g data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchangin g data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchangin g data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchangin g data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 5. Data | Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1. Data Storage - Damage Protection | Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | dynamodb-pitr-enabled | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodica lly. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 7.2. Data Storage - Backups | Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Audit Trails | Consideration should be given, based on a risk assessmen t, to building into the system the creation of a record of all GMP-relev ant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relev ant data the reason should be documente d. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 10. Change and Configuration Management | Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure. | elb-deletion-prote ction-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Change and Configuration Management | Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure. | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 10. Change and Configuration Management | Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. Periodic Evaluation | Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | rds-instance-iam-authentication-enabled | Ensure an AWS Identity and Access Management (IAM) authentication is enabled on Amazon Relational Database Service (Amazon RDS) instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). You are not required to store user credentials in the database, as authentication is managed externally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.1. Security - Authorized Persons | Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.3. Security - Authorization Audit Trail | Creation, change, and cancellation of access authorisations should be recorded. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirmin g or deleting data including date and time. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirmin g or deleting data including date and time. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirmin g or deleting data including date and time. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirmin g or deleting data including date and time. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirmin g or deleting data including date and time. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.4. Security - Audit Trail | Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirmin g or deleting data including date and time. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13. Incident Management | All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13. Incident Management | All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | backup-recovery-po int-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | backup-recovery-po int-minimum-retent ion-check | To help with data back-up processes , ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. This rule allows you to set the requiredRetentionD ays (config default: 35) parameter. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | ebs-optimized-inst ance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/ O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contentio n between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | ebs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | ec2-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | efs-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, container s, and IP addresses , in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | lambda-vpc-multi-az-check | If your AWS Lambda function is configure d to connect to a virtual private cloud (VPC) in your account, deploy the AWS Lambda function in at least two different Availability Zones to ensure that it is your function is available to process events in case of a service interruption in a single zone. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | opensearch-data-no de-fault-tolerance | Amazon OpenSearc h Service (OpenSear ch Service) requires at least three data nodes for high availability and fault-tolerance. Deploying an OpenSearch Service domain with at least three data nodes ensures cluster operations if a node fails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | rds-instance-delet ion-protection-ena bled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | elb-deletion-prote ction-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | rds-cluster-multi-az-enabled | Amazon Relationa l Database Service (Amazon RDS) clusters should have Multi-AZ replicati on enabled to assist in the availability of the data that is stored. Each Availabil ity Zone runs on its own physically distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 16. Business Continuity | For the availability of computerised systems supportin g critical processes , provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (for example a manual or alternative system). The time required to bring the alternati ve arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequatel y documented and tested. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 17. Archiving | Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (for example computer equipment or programs), then the ability to retrieve the data should be ensured and tested. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

### Template

The template is available on GitHub: Operational Best Practices for GxP EU Annex 11.

## Operational Best Practices for HIPAA Security

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Health Insurance Portability and Accountability Act (HIPAA) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more HIPAA controls. A HIPAA control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the HIPAA.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(A) | (A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information | annual-risk-assessment-performed (Process Check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting an organization. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | held by the covered entity. | | |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | dynamodb-throughput-limit-c heck | Enable this rule to ensure that provision ed throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionall y set accountRC UThresholdPercenta ge (Config Default: 80) and accountWC UThresholdPercenta ge (Config Default: 80) parameters. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk managemen t (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(1)(ii)(B) | (B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ecs-containers-rea donly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance' s filesystem cannot be modified unless it has explicit read-writ e permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | codebuild-project-envvar-awscred-che ck | Ensure authentic ation credentials AWS_ACCESS_KEY_ID and AWS_SECRE T_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintende d data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(i) | (3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health informati on, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(A) | (A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedure s to determine that the access of a workforce member to electronic protected health information is appropriate. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(B) | (B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(3)(ii)(C) | (C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | ecs-containers-rea donly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance' s filesystem cannot be modified unless it has explicit read-writ e permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(i) | (4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicabl e requirements of subpart E of this part. | s3-bucket-acl-proh ibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(A) | (A) Isolating health care clearinghouse functions (Required ). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authoriza tion (Addressable). Implement policies and procedures for granting access to electronic protected health informati on, for example, through access to a workstation, transacti on, program, process, or other mechanism. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authoriza tion (Addressable). Implement policies and procedures for granting access to electronic protected health informati on, for example, through access to a workstation, transacti on, program, process, or other mechanism. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authoriza tion (Addressable). Implement policies and procedures for granting access to electronic protected health informati on, for example, through access to a workstation, transacti on, program, process, or other mechanism. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(B) | (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(4)(ii)(C) | (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(5)(ii)(A) | (A) Security reminders (Addressable). Periodic security updates. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 164.308(a)(5)(ii)(A) | (A) Security reminders (Addressable). Periodic security updates. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(A) | (A) Security reminders (Addressable). Periodic security updates. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(A) | (A) Security reminders (Addressable). Periodic security updates. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(B) | (B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(B) | (B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(B) | (B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 164.308(a)(5)(ii)(C) | (C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(5)(ii)(C) | (C) Log-in monitorin g (Addressable). Procedures for monitoring log- in attempts and reporting discrepan cies. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 164.308(a)(5)(ii)(C) | (C) Log-in monitorin g (Addressable). Procedures for monitoring log- in attempts and reporting discrepan cies. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(5)(ii)(D) | (D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(6)(i) | (6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(6)(ii) | (ii) Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(i) | (7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrenc e (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electroni c protected health information. | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electroni c protected health information. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electroni c protected health information. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electroni c protected health information. | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(A) | (A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(B) | (B) Disaster recovery plan (Required ). Establish (and implement as needed) procedures to restore any loss of data. | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| 164.308(a)(7)(ii)(C) | (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuat ion of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(C) | (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuat ion of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 164.308(a)(7)(ii)(C) | (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuat ion of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(C) | (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuat ion of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(C) | (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(7)(ii)(C) | (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(8) | (8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.308(a)(8) | (8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | codebuild-project-envvar-awscred-check | Ensure authentic ation credentials AWS_ACCESS_KEY_ID and AWS_SECRE T_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintende d data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | autoscaling-launch -config-public-ip- disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.308(a)(4). | s3-bucket-acl-proh ibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(1) | (a)(1) Standard: Access control. Implement technical policies and procedures for electronic informati on systems that maintain electroni c protected health information to allow access only to those persons or software programs that have been granted access rights as specified in ¤ 164.308(a)(4). | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(i) | (2) Implementation specifications: (i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedure s for obtaining necessary electroni c protected health information during an emergency. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedure s for obtaining necessary electroni c protected health information during an emergency. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedure s for obtaining necessary electroni c protected health information during an emergency. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedure s for obtaining necessary electroni c protected health information during an emergency. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedure s for obtaining necessary electroni c protected health information during an emergency. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedure s for obtaining necessary electroni c protected health information during an emergency. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedure s for obtaining necessary electroni c protected health information during an emergency. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |
| 164.312(a)(2)(ii) | (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(a)(2)(iv) | (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedura l mechanisms that record and examine activity in informati on systems that contain or use electronic protected health information. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |
| 164.312(b) | (b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(c)(1) | (c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health informati on from improper alteration or destructi on. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| 164.312(c)(1) | (c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health informati on from improper alteration or destructi on. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(c)(1) | (c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health informati on from improper alteration or destructi on. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 164.312(c)(1) | (c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health informati on from improper alteration or destructi on. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(c)(1) | (c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health informati on from improper alteration or destructi on. | opensearch-node-to -node-encryption-c heck | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(c)(2) | (2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(c)(2) | (2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| 164.312(c)(2) | (2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(c)(2) | (2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(c)(2) | (2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(d) | (d) Standard: Person or entity authentic ation. Implement procedures to verify that a person or entity seeking access to electroni c protected health information is the one claimed. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 164.312(d) | (d) Standard: Person or entity authentic ation. Implement procedures to verify that a person or entity seeking access to electroni c protected health information is the one claimed. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(d) | (d) Standard: Person or entity authentic ation. Implement procedures to verify that a person or entity seeking access to electroni c protected health information is the one claimed. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Managemen t (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentia ls. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(d) | (d) Standard: Person or entity authentic ation. Implement procedures to verify that a person or entity seeking access to electroni c protected health information is the one claimed. | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(d) | (d) Standard: Person or entity authentic ation. Implement procedures to verify that a person or entity seeking access to electroni c protected health information is the one claimed. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentia ls. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electroni c protected health information that is being transmitted over an electroni c communications network. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electroni c protected health information that is being transmitted over an electroni c communications network. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electroni c protected health information that is being transmitted over an electroni c communications network. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electroni c protected health information that is being transmitted over an electroni c communications network. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electroni c protected health information that is being transmitted over an electroni c communications network. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electroni c protected health information that is being transmitted over an electroni c communications network. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(1) | (e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(i) | (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electroni c protected health information whenever deemed appropriate. | sagemaker-endpoint -configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electroni c protected health information whenever deemed appropriate. | sagemaker-notebook -instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 164.312(e)(2)(ii) | (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | cloud-trail-encryp tion-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryptio n is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | elasticsearch-encr ypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | opensearch-encrypt ed-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | rds-snapshot-encry pted | Ensure that encryptio n is enabled for your Amazon Relationa l Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(1) | (b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health informati on disclosed to a plan sponsor is disclosed pursuant to ¤ 164.504(f)(1)(ii) or (iii), or as authorized under ¤ 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electroni c protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by ¤ 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | subcontractor, to whom it provides this information agrees to implement reasonabl e and appropriate security measures to protect the informati on; and (iv) Report to the group health plan any security incident of which it becomes aware. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | rds-cluster-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 164.314(b)(2)(i) | (2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to — (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

### Template

The template is available on GitHub: Operational Best Practices for HIPAA Security.

## Operational Best Practices for IRS 1075

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard.

You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the IRS 1075 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more IRS 1075 controls. An IRS 1075 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing d. Data Encryption in Transit | FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.3.1 Cloud Computing d. Data Encryption in Transit | FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | data can exist, enable encryption in transit to help protect that data. |
| 3.3.1 Cloud Computing d. Data Encryption in Transit | FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.3.1 Cloud Computing d. Data Encryption in Transit | FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing d. Data Encryption in Transit | FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.3.1 Cloud Computing d. Data Encryption in Transit | FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing d. Data Encryption in Transit | FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140 certified and operate utilizing the latest FIPS 140 compliant module(s). This requirement must be included in the SLA. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryptio n mechanism. This requirement must be included in the SLA. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryptio n mechanism. This requirement must be included in the SLA. | s3-bucket-server-s ide-encryption-ena bled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryption mechanism. This requirement must be included in the SLA. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryptio n mechanism. This requirement must be included in the SLA. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| 3.3.1 Cloud Computing e. Data Encryption at Rest | Data Encryption at Rest: FTI must be encrypted while at rest in the cloud using the latest FIPS 140 certified encryptio n mechanism. This requirement must be included in the SLA. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing k. Multifactor Authentication | Agencies must implement sufficient multifactor authentication when their cloud solutions are available from the internet (i.e., there is access to the cloud solution from outside of the agency's trusted network). | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing k. Multifactor Authentication | Agencies must implement sufficient multifactor authentication when their cloud solutions are available from the internet (i.e., there is access to the cloud solution from outside of the agency's trusted network). | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 Cloud Computing k. Multifactor Authentication | Agencies must implement sufficient multifactor authentication when their cloud solutions are available from the internet (i.e., there is access to the cloud solution from outside of the agency's trusted network). | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1 Cloud Computing k. Multifactor Authentication | Agencies must implement sufficient multifactor authentication when their cloud solutions are available from the internet (i.e., there is access to the cloud solution from outside of the agency's trusted network). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 3.3.1 Cloud Computing i. Risk Assessment: | The agency must conduct an annual assessment of the security and privacy controls in place on all information systems used for receiving, processing, storing, accessing, protecting and/or transmitting FTI. | annual-risk-assessment-performed(Process Check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting an organization. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | netfw-policy-rule-group-associated | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows, and you define default traffic handling. |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | netfw-stateless-rule-group-not-empty | An AWS Network Firewall rule group contains rules that define how your firewall processes traffic in your VPC. An empty stateless rule group when present in a firewall policy does not process traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no condition s could result in unintended behavior. |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collectio n of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.6 Network Boundary and Infrastructure | Agencies must implement boundary protection devices throughout their system architecture, including routers, firewalls, switches, and intrusion detection systems to protect FTI and FTI systems. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (f) | Create, enable, modify, disable and remove accounts in accordance with agency account management procedures prerequisites; | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (f) | Create, enable, modify, disable and remove accounts in accordance with agency account management procedures prerequisites; | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| AC-2 Account Management (f) | Create, enable, modify, disable and remove accounts in accordance with agency account management procedures prerequisites; | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (f) | Create, enable, modify, disable and remove accounts in accordance with agency account management procedures prerequisites; | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| AC-2 Account Management (f) | Create, enable, modify, disable and remove accounts in accordance with agency account management procedures prerequisites; | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2 Account Management (g) | Monitor the use of accounts | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-2 Account Management (g) | Monitor the use of accounts | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (g) | Monitor the use of accounts | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2 Account Management (g) | Monitor the use of accounts | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2 Account Management (g) | Monitor the use of accounts | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (g) | Monitor the use of accounts | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (g) | Monitor the use of accounts | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (g) | Monitor the use of accounts | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | secretsmanager-secret-periodic-rotation | This rule ensures AWS Secrets Manager secrets have periodic rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. The default value is 90 days. |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 Account Management (j) | Review accounts for compliance with account management requirements | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| (CE-1) Automated System Account Management | Support the management of system accounts using automated mechanisms. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| (CE-1) Automated System Account Management | Support the management of system accounts using automated mechanisms. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| (CE-1) Automated System Account Management | Support the management of system accounts using automated mechanisms. | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| (CE-3): Disable Accounts | Disable accounts within 120 days when the accounts: a. Have expired; b. Are no longer associated to a user or individual; c. Are in violation of organizational policy; or d. Have been inactive for 120 days for non-privileged accounts and 60 days for privileged accounts | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| (CE-12) Account Monitoring for Atypical Usage | Monitor system accounts for agency-defined atypical usage; and Report atypical usage of system accounts to agency-defined personnel or roles. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container’s underlying hardware. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | ecs-containers-non privileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitio ns should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC-6 Least Privilege | Employ the principle of least privilege , allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| AC-17: Remote Access | Establish and document usage restrictions, configura tion/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17: Remote Access | Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| AT-1: Awareness and Training | Provide security and privacy literacy training to system users (including managers, senior executives, and contractors) | security-awareness-program-exists(Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2: Audit Events | Identify the types of events that the system is capable of logging in support of the audit function | audit-log-policy-exists(Process Check) | Establish and maintain an audit log management policy that defines your organization's logging requirements. This includes, but is not limited to, review and retention of audit logs. |
| AU-16: Cross-Organizational Auditing Logging | Employ agency-defined methods for coordinating agency-defined audit information among external organizations when audit information is transmitted across organizational boundaries. | audit-log-policy-exists(Process Check) | Establish and maintain an audit log management policy that defines your organization's logging requirements. This includes, but is not limited to, review and retention of audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7: Continuous Monitoring | Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy: Establish agency-defined metrics to be monitored; Ongoing control assessments in accordance with the continuous monitoring strategy; Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; Correlation and analysis of information generated by control assessments and monitoring; Response actions to address results of the analysis of control assessment and monitoring information; and Reporting the security and privacy | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | status of the system to agency-defined personnel annually, at a minimum. | | |
| CP-9: System Backup | a. Conduct backups of user-level information contained in system documentation, including securityrelated documentation, weekly; b. Conduct backups of system-level information contained in the system weekly; c. Conduct backups of system documentation, including security- and privacy-related documentation weekly; and d. Protect the confidentiality, integrity, and availability of backup information. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-level information contained in system documentation, including securityrelated documentation, weekly; b. Conduct backups of system-level information contained in the system weekly; c. Conduct backups of system documentation, including security- and privacy-related documentation weekly; and d. Protect the confidentiality, integrity, and availability of backup information. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | backup-recovery-po int-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | backup-recovery-po int-minimum-retent ion-check | To help with data back-up processes , ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. This rule allows you to set the requiredRetentionD ays (config default: 35) parameter. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-level information contained in system documentation, including securityrelated documentation, weekly; b. Conduct backups of system-level information contained in the system weekly; c. Conduct backups of system documentation, including security- and privacy-related documentation weekly; and d. Protect the confidentiality, integrity, and availability of backup information. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-level information contained in system documentation, including securityrelated documentation, weekly; b. Conduct backups of system-level information contained in the system weekly; c. Conduct backups of system documentation, including security- and privacy-related documentation weekly; and d. Protect the confidentiality, integrity, and availability of backup information. | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9: System Backup | a. Conduct backups of user-leve l information contained in system documentation, including securityr elated documenta tion, weekly; b. Conduct backups of system-le vel information contained in the system weekly; c. Conduct backups of system documenta tion, including security- and privacy-related documenta tion weekly; and d. Protect the confident iality, integrity, and availability of backup information. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2: Identification and Authentic ation (Organiza tional Users) (CE-1) Multifactor Authentic ation to Privileged Accounts | Implement multi-fac tor authentication for access to privileged accounts | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentia ls. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2: Identification and Authentic ation (Organiza tional Users) (CE-1) Multifactor Authentic ation to Privileged Accounts | Implement multi-fac tor authentication for access to privileged accounts | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2: Identification and Authentication (Organizational Users) (CE-2) Multifactor Authentication to Non-Privileged Accounts | Implement multi-factor authentication for access to non-privileged accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5: Authenticator Management: (CE-1) Password-Based Authentication: For password-based authentication | Enforce the following composition and complexity rules: 1. Enforce minimum password length of fourteen (14) characters. 2. Enforce minimum password complexity to contain a combination of numbers, uppercase letters, lowercase letters, and special characters. 3. Enforce at least one (1) character change when new passwords are selected for use. 4. Store and transmit only cryptogra phically protected passwords. 5. Enforce password lifetime restrictions: i. One (1) day minimum and 90 days maximum. ii. Service accounts passwords shall expire within 366 days (inclusive). | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PM-5: System Inventory | Develop and update continually an inventory of organizational systems. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PM-5: System Inventory | Develop and update continually an inventory of organizational systems. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| PM-5: System Inventory | Develop and update continually an inventory of organizational systems. | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PM-5: System Inventory | Develop and update continually an inventory of organizational systems. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |
| RA-5: Vulnerability Monitoring and Scanning | Monitor and scan for vulnerabilities in the system and hosted applications every thirty (30) days, prior to placing a new information system on the agency network, to confirm remediation actions, and when new vulnerabilities potentially affecting the system are identified and reported | vuln-scans-performed(Process Check) | Ensure vulnerability scans are performed according to your compliance requirements. The cadence of scanning, tools used, and use of results should be defined by your organization. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10: Developer Configuration Management (e.) | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10: Developer Configuration Management (e.) | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10: Developer Configuration Management (e.) | Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10: Developer Configuration Management (a) (c.) | Perform configuration management during system, component, or service design, development, implementation, operation; Implement only organization-approved changes to the system, component, or service; | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4: Information in Shared System Resources | Prevent unauthorized and unintended information transfer from shared system resources | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system component s that are separated from internal organizational networks; and Connect to external networks or informati on systems only through managed interfaces consistin g of boundary protection devices arranged in accordance with an organizational security architecture. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system component s that are separated from internal organizational networks; and Connect to external networks or informati on systems only through managed interfaces consistin g of boundary protection devices arranged in accordance with an organizational security architecture. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system component s that are separated from internal organizational networks; and Connect to external networks or informati on systems only through managed interfaces consistin g of boundary protection devices arranged in accordance with an organizational security architecture. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system component s that are separated from internal organizational networks; and Connect to external networks or informati on systems only through managed interfaces consistin g of boundary protection devices arranged in accordance with an organizational security architecture. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system components that are separated from internal organizational networks; and Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system components that are separated from internal organizational networks; and Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system components that are separated from internal organizational networks; and Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system components that are separated from internal organizational networks; and Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system components that are separated from internal organizational networks; and Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system components that are separated from internal organizational networks; and Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system component s that are separated from internal organizational networks; and Connect to external networks or informati on systems only through managed interfaces consistin g of boundary protection devices arranged in accordance with an organizational security architecture. | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection | Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; Implement subnetworks for publicly accessible system component s that are separated from internal organizational networks; and Connect to external networks or informati on systems only through managed interfaces consistin g of boundary protection devices arranged in accordance with an organizational security architecture. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection (CE-9) Restrict Threatening Outgoing Communications Traffic | Detect and deny outgoing communications traffic posing a threat to external systems; and Audit the identity of internal users associated with denied communications. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection (CE-9) Restrict Threatening Outgoing Communications Traffic | Detect and deny outgoing communications traffic posing a threat to external systems; and Audit the identity of internal users associated with denied communications. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| SC-7: Boundary Protection (CE-9) Restrict Threatening Outgoing Communications Traffic | Detect and deny outgoing communications traffic posing a threat to external systems; and Audit the identity of internal users associated with denied communications. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7: Boundary Protection (IRS-Defined) | Agencies shall implement and manage boundary protection (typically using firewalls) at trust boundaries. Each trust boundary shall be monitored and communications across each boundary shall be controlled. | netfw-policy-rule-group-associated | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows, and you define default traffic handling. |
| SC-7: Boundary Protection (IRS-Defined) | Agencies shall implement and manage boundary protection (typically using firewalls) at trust boundaries. Each trust boundary shall be monitored and communications across each boundary shall be controlled. | netfw-stateless-rule-group-not-empty | An AWS Network Firewall rule group contains rules that define how your firewall processes traffic in your VPC. An empty stateless rule group when present in a firewall policy does not process traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8: Transmission Confidentiality and Integrity (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8: Transmission Confidentiality and Integrity (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8: Transmission Confidentiality and Integrity (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8: Transmission Confidentiality and Integrity (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8: Transmission Confidentiality and Integrity (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8: Transmission Confidentiality and Integrity (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8: Transmission Confidentiality and Integrity (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-12: Cryptographic Key Establishment and Management | The agency must establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: NIST SP 800-57, Recommendation for Key Management, for key generation, distribution, storage, access, and destruction. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12: Cryptographic Key Establishment and Management | The agency must establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: NIST SP 800-57, Recommendation for Key Management, for key generation, distribution, storage, access, and destruction. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptography required for each specified cryptographic use: Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 for digital signatures is prohibited. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13: Cryptographic Protection | Implement the following types of cryptogra phy required for each specified cryptographic use: Latest FIPS-140 validated encryptio n mechanism, NIST 800-52, Guideline s for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryptio n). Use of SHA-1 for digital signatures is prohibited. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23: Session Authenticity | Protect the authenticity of communications sessions. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SC-28: Protection of Information at Rest (CE-1) Cryptographic Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of FTI at rest on end user computing systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2: Flaw Remediation (IRS-Defined) | The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than after every 24 hours (excluding weekends, holidays, etc.) | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2: Flaw Remediation (IRS-Defined) | The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than after every 24 hours (excluding weekends, holidays, etc.) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2: Flaw Remediation (IRS-Defined) | The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than after every 24 hours (excluding weekends, holidays, etc.) | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2: Flaw Remediati on (IRS-Defined) | The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than after every 24 hours (excluding weekends, holidays, etc.) | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2: Flaw Remediation (IRS-Defined) | The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than after every 24 hours (excluding weekends, holidays, etc.) | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2: Flaw Remediation (IRS-Defined) | The agency shall ensure that, upon daily power up and connection to the agency's network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than after every 24 hours (excluding weekends, holidays, etc.) | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring | The organization: a. Monitors the information system to detect: 1.Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2.Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c.Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d.Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring | The organization: a. Monitors the information system to detect: 1.Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2.Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c.Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d.Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring | The organization: a. Monitors the information system to detect: 1.Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2.Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c.Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d.Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring | The organization: a. Monitors the information system to detect: 1.Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2.Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c.Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | d.Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring | The organization: a. Monitors the information system to detect: 1.Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2.Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c.Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | d.Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; | | |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4: System Monitoring (IRS-Defined) | All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7: Software, Firmware and Information Integrity | Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: system kernels, drivers, firmware (for example, BIOS, UEFI), software (for example, OS, applications, middleware) and security attributes. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7: Software, Firmware and Information Integrity | Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: system kernels, drivers, firmware (for example, BIOS, UEFI), software (for example, OS, applications, middleware) and security attributes. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7: Software, Firmware and Information Integrity | Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: system kernels, drivers, firmware (for example, BIOS, UEFI), software (for example, OS, applications, middleware) and security attributes. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | dynamodb-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | ebs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | efs-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | rds-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | s3-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| SI-12: Information Management and Retention | Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

### Template

The template is available on GitHub: Operational Best Practices for IRS 1075.

## Operational Best Practices for K-ISMS

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between Korea – Information Security Management System (ISMS) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more Korea – ISMS controls. A Korea – ISMS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2.1 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 1.2.1 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| 2.1.3 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.1.3 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |
| 2.3.3 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 2.3.3 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 2.5.1 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 2.5.1 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| 2.5.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 2.5.1 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.1 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 2.5.3 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.3 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 2.5.3 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5.4 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
|---|---|---|
| | | actual values should reflect your organization's policies. |
| 2.5.5 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 2.5.5 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 2.5.5 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| 2.6 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 2.6 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 2.6 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 2.6 | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 2.6 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 2.6 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organization's policies. |
| 2.6 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 2.6 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 2.6 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 2.6 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 2.6.6 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6.6 | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 2.6.6 | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| 2.6.6 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6.6 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 2.6.6 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6.6 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 2.6.6 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6.6 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 2.6.6 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 2.6.6 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.6.6 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 2.6.7 | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 2.7 | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configure d to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.7 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 2.7 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 2.7 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 2.7 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | ec2-ebs-encryption-by-defau lt | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 2.7 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 2.7 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.7 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 2.7 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 2.7 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| 2.7 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 2.7 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 2.7 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.7 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| 2.7 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| 2.7 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.7.1 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7.1 | elb-predefined-security-policy-ssl-check | To help protect data in transit, ensure that your Classic Elastic Load Balancing SSL listeners are using a predefined security policy. Elastic Load Balancing provides predefined SSL negotiation configurations that are used for SSL negotiation when a connection is established between a client and your load balancer. The SSL negotiation configurations provide compatibility with a broad range of clients and use high-strength cryptographic algorithms. This rule requires that you set a predefined security policy for your SSL listeners. The default security policy is: ELBSecurityPolicy-TLS-1-2-2017-0. The actual value should reflect your organization's policies |
| 2.7.2 | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.7.2 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| 2.8.5 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.8.5 | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |
| 2.8.6 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.8.6 | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |
| 2.9.1 | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 2.9.1 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.1 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.1 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.2 | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.2 | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.2 | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughpu t capacity is checked on your Amazon DynamoDB tables. This is the amount of read/ write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approache s the maximum limit for a customer's account. This rule allows you to optionall y set accountRCUThreshol dPercentage (Config Default: 80) and accountWCUThreshol dPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |
| 2.9.2 | ec2-instance-detailed-monit oring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.2 | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| 2.9.2 | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| 2.9.3 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 2.9.3 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 2.9.3 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 2.9.3 | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 2.9.3 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |
| 2.9.3 | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 2.9.3 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.3 | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |
| 2.9.3 | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.4 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 2.9.4 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 2.9.4 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 2.9.4 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.4 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 2.9.4 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.4 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| 2.9.4 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.4 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 2.9.4 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.9.4 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 2.10.3 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.10.3 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 2.10.3 | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.10.3 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 2.10.3 | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 2.10.5 | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.10.5 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.10.5 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.10.5 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.10.5 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.10.5 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/ SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.10.5 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.10.5 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.10.8 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.10.8 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 2.11.2 | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.11.3 | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |
| 2.11.3 | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.11.3 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 2.11.3 | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.11.3 | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.11.3 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 2.12 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| 2.12 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 2.12 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 2.12 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 2.12 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 2.12 | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| 2.12 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| 2.12 | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.12 | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

### Template

The template is available on GitHub: Operational Best Practices for K-ISMS.

## Operational Best Practices for Load Balancing

This conformance pack contains AWS Config rules based on load balancing within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Load Balancing.

## Operational Best Practices for Logging

This conformance pack contains AWS Config rules based on logging within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Logging.

## Operational Best Practices for Management and Governance Services

This conformance pack contains AWS Config rules based on Management and Governance Services. For more information, see Management and Governance on AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Management and Governance Services.

## Operational Best Practices for MAS Notice 655

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Monetary Authority of Singapore (MAS) Notice 655 – Cyber Hygiene and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more MAS Notice 655 – Cyber Hygiene controls. A MAS Notice 655 – Cyber Hygiene control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |
| 4.1 | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |
| 4.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 4.1 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 4.1 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 4.1 | root-account-hardware-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 4.1 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 4.1 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| 4.1 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |
| 4.1 | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| 4.1 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.2 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 4.2 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.2 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.2 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 4.2 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.2 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 4.2 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| 4.2 | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.3 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 4.3 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.3 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 4.3 | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant . The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |
| 4.4 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 4.4 | ebs-snapshot-public-restora ble-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 4.4 | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| 4.4 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 4.4 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 4.4 | lambda-function-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 4.4 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 4.4 | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no conditions could result in unintended behavior. |
| 4.4 | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |
| 4.4 | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collection of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | netfw-policy-default-action-fragment-packets | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows. Defaulting to a Pass action may allow unintended traffic. |
| 4.4 | netfw-policy-default-action-full-packets | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows. Defaulting to a Pass action may allow unintended traffic. |
| 4.4 | netfw-policy-rule-group-associated | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows, and you define default traffic handling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | netfw-stateless-rule-group-not-empty | An AWS Network Firewall rule group contains rules that define how your firewall processes traffic in your VPC. An empty stateless rule group when present in a firewall policy does not process traffic. |
| 4.4 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 4.4 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 4.4 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| 4.4 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 4.4 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 4.4 | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 4.4 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| 4.4 | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 4.4 | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 4.4 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.4 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| 4.5 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applicati ons within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.5 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 4.5 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.5 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.6 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 4.6 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 4.6 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.6 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 4.6 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.6 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

### Template

The template is available on GitHub: Operational Best Practices for MAS Notice 655.

## Operational Best Practices for MAS TRMG

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Monetary Authority of Singapore (MAS) Technology Risk Managment Guidelines (TRMG) January 2021 and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more MAS TRMG controls. A MAS TRMG January 2021 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 3.3.1 | account-part-of-organizations | Centralized management of AWS accounts within AWS |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | Organizations helps to ensure that accounts are compliant . The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 5.4.3 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| 5.4.3 | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.1.1 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| 6.1.2 | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.1.4 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 6.1.4 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.1.4 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 6.2.1 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 6.3.1 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.5 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 6.4.5 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 6.4.5 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 6.4.5 | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.5 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 6.4.5 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 6.4.5 | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.5 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 6.4.5 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 6.4.5 | elbv2-acm-certificate-requi red | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.5 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 6.4.5 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 6.4.6 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 6.4.6 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.6 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 6.4.6 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.6 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.6 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| 6.4.6 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.6 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.6 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 6.4.6 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.7 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 6.4.7 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 6.4.7 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.7 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 6.4.7 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.7 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| 6.4.7 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 6.4.7 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.7 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 6.4.7 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.7 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 6.4.7 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.7 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 6.4.7 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.7 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 6.4.8 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provision ed throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.8 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 6.4.8 | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.8 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 6.4.8 | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 6.4.8 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.8 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4.8 | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implement ed to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-Site VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.2.1 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 7.2.1 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.4.1 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 7.4.1 | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.4.1 | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 7.4.1 | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| 7.4.1 | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.4.1 | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |
| 7.5.5 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.5 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 7.5.5 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.5 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 7.5.5 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.5 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 7.5.5 | rds-in-backup-plan | To help with data backup processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.5 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 7.5.5 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.5 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| 7.5.7 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 7.5.7 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.7 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 7.5.7 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 7.5.7 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.7 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 7.5.7 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 7.5.7 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.7 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.7 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 7.5.7 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 7.5.7 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| 8.1.1 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.1 | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |
| 8.1.1 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.1 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 8.1.1 | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 8.1.1 | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.1 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.1 | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |
| 8.1.2 | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.2 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.2 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 8.1.2 | opensearch-data-node-fault-tolerance | Amazon OpenSearch Service (OpenSearch Service) requires at least three data nodes for high availability and fault-tolerance. Deploying an OpenSearch Service domain with at least three data nodes ensures cluster operations if a node fails. |
| 8.1.2 | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.3 | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |
| 8.1.3 | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.1.3 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 8.1.3 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 8.4.1 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.1 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 8.4.1 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.1 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 8.4.1 | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.1 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 8.4.1 | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requireme nts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.1 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 8.4.1 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.1 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 8.4.1 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.2 | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| 8.4.2 | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.2 | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| 8.4.2 | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.2 | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 8.4.2 | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.2 | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 8.4.2 | rds-in-backup-plan | To help with data backup processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.2 | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 8.4.2 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.4.2 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| 8.4.4 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.5.4 | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchrono usly replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 8.5.4 | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 9.1.1 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 9.1.1 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 9.1.1 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 9.1.1 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 9.1.1 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authoriza tions, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 9.1.1 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| 9.1.1 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 9.1.1 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 9.1.1 | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| 9.1.1 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| 9.1.1 | secretsmanager-secret-periodic-rotation | This rule ensures AWS Secrets Manager secrets have periodic rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. The default value is 90 days. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.1 | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.2 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.2 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.2 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.2 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| 9.1.2 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.2 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 9.1.3 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 9.1.3 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 9.1.3 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.3 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 9.1.3 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.3 | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| 9.1.3 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 9.1.3 | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.3 | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 9.1.3 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| 9.1.3 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.3 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| 9.1.3 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.3 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.3 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 9.1.3 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.3 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 9.1.3 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.4 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 9.1.5 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 9.1.5 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.5 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 9.1.5 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.6 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.7 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.7 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.7 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.7 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.1.7 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| 9.1.7 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 9.2.1 | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.1 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 9.2.1 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 9.2.1 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 9.2.1 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.1 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrai l logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrai l delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 9.2.1 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.1 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 9.2.1 | multi-region-cloudtrail-ena bled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containin g API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.1 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.1 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 9.2.2 | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 9.2.2 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.2 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 9.2.2 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 9.2.2 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.2 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 9.2.2 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.2 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 9.2.2 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.2 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.2.2 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 9.3.1 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 9.3.1 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.3.1 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 9.3.1 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.3.1 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 9.3.1 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.3.1 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 9.3.1 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 9.3.1 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.3.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| 9.3.1 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.3.1 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 9.3.1 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 9.3.1 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 9.3.1 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 10.1.1 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 10.1.1 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 10.1.1 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 10.1.1 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 10.1.1 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 10.1.1 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 10.1.1 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 10.1.1 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 10.1.1 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 10.1.1 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 10.1.1 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 10.1.1 | elbv2-acm-certificate-requi red | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 10.1.1 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| 10.1.1 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 10.1.1 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 10.1.1 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 10.1.1 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 10.1.1 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 10.1.1 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.1.1 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 10.1.1 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| 10.2.1 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.2.1 | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |
| 10.2.1 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| 10.2.2 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 10.2.3 | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |
| 10.2.3 | cmk-backing-key-rotation-en abled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |
| 10.2.3 | kms-cmk-not-scheduled-for-d eletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (a) | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 11.1.1 (a) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 11.1.1 (a) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (a) | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 11.1.1 (a) | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 11.1.1 (a) | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (a) | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 11.1.1 (a) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 11.1.1 (a) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (a) | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 11.1.1 (b) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 11.1.1 (b) | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 11.1.1 (b) | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 11.1.1 (b) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 11.1.1 (b) | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 11.1.1 (b) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 11.1.1 (b) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 11.1.1 (b) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 11.1.1 (b) | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 11.1.1 (b) | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| 11.1.1 (b) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 11.1.1 (b) | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 11.1.1 (b) | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| 11.1.1 (b) | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestric ted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 11.1.1 (b) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 11.1.1 (b) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 11.1.1 (b) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 11.1.1 (b) | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 11.1.1 (b) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 11.1.1 (b) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 11.1.1 (b) | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 11.1.1 (b) | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 11.1.1 (b) | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| 11.1.1 (b) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 11.1.1 (b) | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| 11.1.1 (b) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.1 (b) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 11.1.3 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 11.1.3 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 11.1.3 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 11.1.3 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 11.1.3 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 11.1.3 | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpecte d privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| 11.1.3 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 11.1.3 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 11.1.3 | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authentic ate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principal s to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative information about each principal. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 11.1.3 | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 11.1.3 | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authoriza tions, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 11.1.3 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 11.1.3 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| 11.1.3 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryptio n at rest to help protect that data. |
| 11.1.3 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 11.1.3 | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 11.1.3 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 11.1.3 | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 11.1.3 | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 11.1.3 | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.1.3 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 11.1.3 | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| 11.2.1 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 11.2.2 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 11.2.2 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 11.2.2 | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connectio n. |
| 11.2.2 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 11.2.2 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |
| 11.2.2 | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 11.2.2 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 11.2.2 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 11.2.2 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 11.2.2 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 11.2.2 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.2 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| 11.2.2 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 11.2.4 | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 11.2.4 | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 11.2.4 | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 11.2.4 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |
| 11.2.4 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| 11.2.4 | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |
| 11.2.4 | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 11.2.4 | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| 11.2.4 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthori zed users. |
| 11.2.4 | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| 11.2.4 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.2.4 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 11.3.1 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.3.5 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 11.3.5 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.3.5 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.3.5 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 11.4.2 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.4.2 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organization's policies. |
| 11.4.2 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 11.4.2 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 11.5.2 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.1.1 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 12.1.1 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.1.1 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.1.1 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 12.2.2 | api-gw-execution-logging-en abled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 12.2.2 | cloud-trail-cloud-watch-logs- enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.2 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 12.2.2 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 12.2.2 | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.2 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 12.2.2 | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 12.2.2 | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.2 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 12.2.2 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.2 | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 12.2.2 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.2 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| 12.2.2 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.2 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 12.2.2 | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.4 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 12.2.4 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.5 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 12.2.5 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.5 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.2.5 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 12.3.2 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.3.2 | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 12.3.2 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 14.1.2 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 14.1.2 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.1.2 | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 14.1.2 | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.1.2 | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 14.1.2 | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 14.1.2 | elbv2-acm-certificate-requi red | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.1.2 | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 14.1.2 | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 14.1.3 | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applicati ons or APIs against common web exploits. These web exploits may affect availabil ity, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.1.3 | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| 14.1.3 | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.1.3 | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregate s, organizes, and prioritiz es the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 14.2.2 | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.2.2 | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 14.2.2 | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 14.2.2 | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.2.2 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 14.2.2 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 14.2.2 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 14.2.2 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.2.2 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 14.2.2 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 14.2.2 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.2.2 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 14.2.6 | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.2.6 | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 14.2.6 | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 14.2.6 | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 14.2.6 | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.2.6 | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryptio n at rest to help protect that data. |
| 14.2.6 | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 14.2.6 | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

### Template

The template is available on GitHub: Operational Best Practices for MAS TRMG.

## Operational Best Practices for Monitoring

This conformance pack contains AWS Config rules based on monitoring within AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Monitoring.

# Operational Best Practices for NBC TRMG

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the National Bank of Cambodia's (NBC) Technology Risk Management (TRM) Guidelines framework and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NBC TRM Guideline. An NBC TRM Guideline can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the National Bank of Cambodia's (NBC) Technology Risk Management (TRM) Guidelines framework, which can be accessed here: National Bank of Cambodia: Technology Risk Management Guidelines.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implement ation of role-base d access control | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modificat ion of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all | | principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implement ation of role-base d access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modificat ion of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implement ation of role-base d access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modificat ion of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implement ation of role-base d access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modificat ion of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implement ation of role-base d access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modificat ion of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implement ation of role-base d access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modificat ion of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(d) | d) Among the important controls that need to be considered are: - A systematic process of applying and authorising the creation of user IDs and the access control matrix - Conducting a risk assessment and granting access rights based on the same. - Implementation of role-based access control designed to ensure effective segregation of duties - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/ | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | contract - Processes to notify in a timely manner the informati on security function regarding user addi tions, deletions and role changes - Periodic reconcili ation of user IDs in a system and actual users required to have access and deletion of any unnecessa ry IDs, if any - Auditing, logging and monitoring of access to IT assets by all users and - Consideri ng de-activating user IDs of users of critical applications who are on prolonged leave | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(f) | f) For accountability purpose, ensure that users and IT assets are uniquely identifie d and their actions are auditable. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(f) | f) For accountability purpose, ensure that users and IT assets are uniquely identified and their actions are auditable. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(f) | f) For accountability purpose, ensure that users and IT assets are uniquely identified and their actions are auditable. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 3.1.1(f) | f) For accountability purpose, ensure that users and IT assets are uniquely identified and their actions are auditable. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(f) | f) For accountability purpose, ensure that users and IT assets are uniquely identifie d and their actions are auditable. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(f) | f) For accountability purpose, ensure that users and IT assets are uniquely identifie d and their actions are auditable. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 3.1.1(f) | f) For accountability purpose, ensure that users and IT assets are uniquely identifie d and their actions are auditable. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | data from unauthori sed access | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1(h) | h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered: - Implementing two-factor authentication for privileged users - Instituti | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ng strong controls over remote access by privileged users - Restricting the number of privilege d users - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis - Maintaining audit logging of system activities performed by privileged users - Ensuring that privileged users do not have access to systems logs in which their activities are being captured - Conducting regular audit or managemen t review of the logs - Prohibiting sharing of privileged IDs and their access codes - Disallowing vendors and contracto rs from gaining privileged access to systems without close supervision and monitoring and _ Protecting backup | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | data from unauthori sed access | | |
| 3.1.2(a) | a) The BFI should install network security devices, such as firewalls, anti-virus/anti-malware software as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure, to protect the network perimeters. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| 3.1.2(a) | a) The BFI should install network security devices, such as firewalls, anti-virus/anti-malware software as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure, to protect the network perimeters. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(a) | a) The BFI should install network security devices, such as firewalls, anti-virus/anti-malware software as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure, to protect the network perimeters. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considere d: - Responsibilities and procedures for the managemen t of networking equipment should be established - Operational responsibility for networks should be separated from computer operation s where appropriate - Special controls should be establish ed to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(c) | c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered: - Responsibilities and procedures for the management of networking equipment should be established - Operational responsibility for networks should be separated from computer operations where appropriate - Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (include network encryption protocols when connectin g to untrusted systems/ networks. - Appropriate logging and monitoring should be applied to enable recording and detection of action s that may affect, or are relevant to, information security - Management activitie s should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consisten tly applied across the information proces sing infrastructure - Systems on the network should be authenticated and - Untrusted system connections to the network should be restricted | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | alb-http-drop-inva lid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentication, encryption and network connection controls - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and - Procedures for the network service usage to restrict access to network services or applications, where necessary | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2(e) | e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be: - Technology applied for security of network services, such as authentic ation, encryption and network connection controls - Technical parameters required for secured connectio n with the network services in accordance with the security and network connection rules and - Procedure s for the network service usage to restrict access to network services or applications, where necessary | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 3.1.3(e) | e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 3.1.3(g) | g) Maintain logs for remote access communications. Logs should include the date, time, user, user loca tion, duration, and purpose for all remote access including all activities carried out through r emote access | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(i) | i)Enforce two-factor authentication process for remote access (for example, PIN based token card with a one-time random password generator, or token based PKI) | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(i) | i)Enforce two-factor authentication process for remote access (for example, PIN based token card with a one-time random password generator, or token based PKI) | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(i) | i)Enforce two-factor authentication process for remote access (for example, PIN based token card with a one-time random password generator, or token based PKI) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3(i) | i)Enforce two-factor authentication process for remote access (for example, PIN based token card with a one-time random password generator, or token based PKI) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, for example automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | failed deployment of a patch (for example, redeployment of the patch). e ) BFIs should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, for example automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | failed deploymen t of a patch (for example, redeploym ent of the patch). e ) BFIs should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.4(c)(e) | c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, for example automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | failed deploymen t of a patch (for example, redeploym ent of the patch). e ) BFIs should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, for example automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | failed deployment of a patch (for example, redeployment of the patch). e ) BFIs should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.4(c)(e) | c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, for example automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | failed deployment of a patch (for example, redeployment of the patch). e ) BFIs should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4(c)(e) | c) The patch management process should include aspects like: - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source - Identifying vulnerabilities that are applicable to applications and systems used by the organisation - Assessing the business impact of implementing patches (or not implementing a particular patch) - Ensuring patches are tested - Describing methods for deploying patches, for example automatically - Reporting on the status of patch deployment across the organisation and - Including methods for dealing with the | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | failed deploymen t of a patch (for example, redeploym ent of the patch). e ) BFIs should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe | | |
| 3.1.5(d)(e) | d) Appropriate key management requires secure processes for generating, storing, archiving, retriev ing, distributing, retiring and destroyin g cryptographic keys e) All cryptogra phic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosur e. Equipment used to generate, store and archive keys should be physically protected | kms-cmk-not-schedu led-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5(d)(e) | d) Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys e) All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5(d)(e) | d) Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys e) All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5(d)(e) | d) Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys e) All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5(f) | f) A key managemen t system should be based on an agreed set of standards , procedures and secure methods for: - generating keys for different cryptogra phic systems and different applicati ons - issuing and obtaining public key certificates - distribut ing keys to intended entities, including how keys should be activated when received - storing keys, including how authorised users obtain access to keys - changing or updating keys including rules on when keys should be changed and how this will be done - dealing with compromised keys - revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromis | kms-cmk-not-schedu led-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ed or when a user leaves an organisat ion (in which case keys should also be archived) - recoverin g keys that are lost or corrupted - backing up or archiving keys - destroying keys, and - logging and auditing of key management related activities. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5(f) | f) A key managemen t system should be based on an agreed set of standards , procedures and secure methods for: - generating keys for different cryptogra phic systems and different applicati ons - issuing and obtaining public key certificates - distribut ing keys to intended entities, including how keys should be activated when received - storing keys, including how authorised users obtain access to keys - changing or updating keys including rules on when keys should be changed and how this will be done - dealing with compromised keys - revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromis | cmk-backing-key-ro tation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ed or when a user leaves an organisat ion (in which case keys should also be archived) - recoverin g keys that are lost or corrupted - backing up or archiving keys - destroying keys, and - logging and auditing of key management related activities. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5(f) | f) A key managemen t system should be based on an agreed set of standards , procedures and secure methods for: - generating keys for different cryptogra phic systems and different applicati ons - issuing and obtaining public key certificates - distribut ing keys to intended entities, including how keys should be activated when received - storing keys, including how authorised users obtain access to keys - changing or updating keys including rules on when keys should be changed and how this will be done - dealing with compromised keys - revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromis | acm-certificate-ex piration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundatio nal Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ed or when a user leaves an organisat ion (in which case keys should also be archived) - recoverin g keys that are lost or corrupted - backing up or archiving keys - destroying keys, and - logging and auditing of key management related activities. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5(f) | f) A key managemen t system should be based on an agreed set of standards , procedures and secure methods for: - generating keys for different cryptogra phic systems and different applicati ons - issuing and obtaining public key certificates - distribut ing keys to intended entities, including how keys should be activated when received - storing keys, including how authorised users obtain access to keys - changing or updating keys including rules on when keys should be changed and how this will be done - dealing with compromised keys - revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromis | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ed or when a user leaves an organisat ion (in which case keys should also be archived) - recoverin g keys that are lost or corrupted - backing up or archiving keys - destroying keys, and - logging and auditing of key management related activities. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5(f) | f) A key managemen t system should be based on an agreed set of standards , procedures and secure methods for: - generating keys for different cryptogra phic systems and different applicati ons - issuing and obtaining public key certificates - distribut ing keys to intended entities, including how keys should be activated when received - storing keys, including how authorised users obtain access to keys - changing or updating keys including rules on when keys should be changed and how this will be done - dealing with compromised keys - revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromis | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ed or when a user leaves an organisat ion (in which case keys should also be archived) - recoverin g keys that are lost or corrupted - backing up or archiving keys - destroying keys, and - logging and auditing of key management related activities. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5(f) | f) A key managemen t system should be based on an agreed set of standards , procedures and secure methods for: - generating keys for different cryptogra phic systems and different applicati ons - issuing and obtaining public key certificates - distribut ing keys to intended entities, including how keys should be activated when received - storing keys, including how authorised users obtain access to keys - changing or updating keys including rules on when keys should be changed and how this will be done - dealing with compromised keys - revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromis | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ed or when a user leaves an organisat ion (in which case keys should also be archived) - recoverin g keys that are lost or corrupted - backing up or archiving keys - destroying keys, and - logging and auditing of key management related activities. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5(f) | f) A key managemen t system should be based on an agreed set of standards , procedures and secure methods for: - generating keys for different cryptogra phic systems and different applicati ons - issuing and obtaining public key certificates - distribut ing keys to intended entities, including how keys should be activated when received - storing keys, including how authorised users obtain access to keys - changing or updating keys including rules on when keys should be changed and how this will be done - dealing with compromised keys - revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromis | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ed or when a user leaves an organisat ion (in which case keys should also be archived) - recoverin g keys that are lost or corrupted - backing up or archiving keys - destroying keys, and - logging and auditing of key management related activities. | | |
| 3.1.6(a) | a) The BFI should deploy a combinati on of automated tools and manual techniques to perform a compreh ensive VA on a periodic basis. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.6(a) | a) The BFI should deploy a combination of automated tools and manual techniques to perform a comprehensive VA on a periodic basis. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| 3.1.6(a) | a) The BFI should deploy a combination of automated tools and manual techniques to perform a comprehensive VA on a periodic basis. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.6(c) | c) The BFI should establish a process to remediate the issues identifie d in VA & PT and perform subsequen t revalidation of the remediation to validate that gaps are fully addressed. | vuln-mitigated-acc epted(Process Check) | Ensure newly identified vulnerabi lities are remediate d or documented as accepted risks. Vulnerabilities should be remediate d or accepted as risks according to your organizat ions compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.6(f) | f) The security function should provide status updates regarding the number of unmitigated, critical vulnerabilities, for each department/ division, and plan for mitigating to senior management on a periodic basis | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.8 | User training and awareness | security-awareness-program-exists(Process Check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive informati on such as system documentation, application source code, and productio n transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptogra phic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive informati on such as system documentation, application source code, and productio n transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptogra phic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.10(b) | b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (for example, integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former ve rsion of the system or application if a problem is encounter ed during or after the deployment. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former ve rsion of the system or application if a problem is encounter ed during or after the deployment. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former ve rsion of the system or application if a problem is encounter ed during or after the deployment. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former ve rsion of the system or application if a problem is encounter ed during or after the deployment. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former ve rsion of the system or application if a problem is encounter ed during or after the deployment. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former ve rsion of the system or application if a problem is encounter ed during or after the deployment. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former ve rsion of the system or application if a problem is encounter ed during or after the deployment. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.2.1(h) | h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and troubleshooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investiga tions and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investiga tions and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investiga tions and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investiga tions and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investiga tions and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 3.2.1(k) | k) Audit and security logs are useful information which facilitates investiga tions and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.3(a) | a) Develop and implement processes for preventing, detecting, analysing and responding to information security incidents. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.3(a) | a) Develop and implement processes for preventing, detecting, analysing and responding to information security incidents. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | dynamodb-autoscali ng-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/writ e capacity to handle sudden increases in traffic, without throttling. |
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1(a) | a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 3.3.1(a) | a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1(a) | a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 3.3.1(a) | a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | dynamodb-throughput-limit-check | Enable this rule to ensure that provision ed throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionall y set accountRC UThresholdPercenta ge (Config Default: 80) and accountWC UThresholdPercenta ge (Config Default: 80) parameters. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1(a) | a) Consider important factors associate d with maintaini ng high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design. | lambda-concurrency-check | This rule ensures that a Lambda function' s concurrency high and low limits are established. This can assist in baselinin g the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(a)(b)(c)(f)(j) | a) Ensure that records of user access are uniquely identified and logged for audit and review purposes. b) Have accountability and identification of unauthorised access is documented. c) Enable audit logging of system activities performed by privileged users. f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(f) | f) Ensure appropria te logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activitie s - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successfu l and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transacti ons executed by users in applications and online customer transaction | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activitie s - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successfu l and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transacti ons executed by users in applications and online customer transaction | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activitie s - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successfu l and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transacti ons executed by users in applications and online customer transaction | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activitie s - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successfu l and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transacti ons executed by users in applications and online customer transaction | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activities - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successful and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transactions executed by users in applications and online customer transaction | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activitie s - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successfu l and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transacti ons executed by users in applications and online customer transaction | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4(g) | g) Ensure event logs include, when relevant: - User IDs - System activitie s - Dates, time and details of key events, for example log-on and log-off - Device identity or location if possible and system identifier - Records of successful and rejected system access attempts - Records of successfu l and rejected data and other resource access attempts - Changes to system configuration - Use of privileges - Use of system utilities and applications - Files accessed and the kind of access - Network addresses and protocols - Alarms raised by the access control system and - Records of transacti ons executed by users in applications and online customer transaction | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.1(a)(h) | a) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks. h) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| 3.6.1(a)(h) | a) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks. h) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryptio n solution consideri ng the degree of confidentiality and integrity required. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryptio n solution consideri ng the degree of confidentiality and integrity required. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 3.6.1(b) | b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(d) | d) BFIs providing internet banking should be responsiv e to unusual network traffic conditions/ system performan ce and sudden surge in system resource utilisation which could be an indicatio n of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deploymen t of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(d) | d) BFIs providing internet banking should be responsiv e to unusual network traffic conditions/ system performan ce and sudden surge in system resource utilisation which could be an indicatio n of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deploymen t of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(d) | d) BFIs providing internet banking should be responsiv e to unusual network traffic conditions/ system performan ce and sudden surge in system resource utilisation which could be an indicatio n of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deploymen t of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(d) | d) BFIs providing internet banking should be responsiv e to unusual network traffic conditions/ system performan ce and sudden surge in system resource utilisation which could be an indicatio n of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deploymen t of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(d) | d) BFIs providing internet banking should be responsiv e to unusual network traffic conditions/ system performan ce and sudden surge in system resource utilisation which could be an indicatio n of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deploymen t of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1(e) | e) BFIs need to regularly assess information security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, making any necessary adjustments to ensure emerging vulnerabilities are addressed in a timely manner. This assessment should also be conducted as part of any material change. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environme nt. b) Reduce attack surface and vulnerabi lities. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4(a)(b) | a) Restrict internet access & segregate critical systems from General IT environment. b) Reduce attack surface and vulnerabilities. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

### Template

The template is available on GitHub: Operational Best Practices for NBC TRMG.

## Operational Best Practices for NERC CIP BCSI

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) for BES Cyber System Information (BCSI), CIP-004-7 & CIP-011-3, and AWS Config managed rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more NERC CIP controls applicable to BCSI. A NERC CIP control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch dashboards multi-tenancy, and HTTP basic authentication for OpenSearch and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-004-7-R6-Part 6.1 | Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the “Applicable Systems” identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-7 Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | an individual(s) the means to access BCSI (for example, may include physical keys or access cards, users and associated rights and privileges, encryption keys). Part 6.1: Prior to provision ing, authorize (unless already authorize d according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electroni c access to electronic BCSI | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | ecr-private-tag-immutability-enabled | Enable Elastic Container Repository (ECR) Tag Immutability to prevent image tags on your ECR images from being overwritten. Previously, tags could be overwritten requiring manual methodologies to uniquely identify an image. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | s3-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | rds-cluster-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Relational Database Service (Amazon RDS) database cluster(s). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | rds-instance-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Relational Database Service (Amazon RDS) database instance(s). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | redshift-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Redshift cluster(s). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CIP-011-3-R1-Part 1.2 | Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection. Part 1.2: Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

### Template

The template is available on GitHub: Operational Best Practices for NERC CIP BCSI.

## Operational Best Practices for NCSC Cloud Security Principles

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the UK National Cyber Security Centre (NCSC) Cloud Security Principles and AWS managed Config rules. Each Config rule applies to a specific

AWS resource, and relates to one or more UK NCSC Cloud Security Principles controls. A UK NCSC Cloud Security Principles control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the UK NCSC Cloud Security Principles (National Cyber Security Centre | Cloud security guidance), with such public sector information licensed under the Open Government Licence v3.0. The Open Government Licence should can be accessed here: Open Government Licence for public sector information.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundatio |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | nal Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1. Data in transit protection | User data transiting networks should be adequately protected against tampering and eavesdropping. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 2. Asset protection and resilience | Your data (and the assets storing or processing it) should be adequately protected. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5. Operational security | Services must be operated and managed in a way to impede, detect or prevent attacks. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7. Secure development | Cloud services should be designed, developed and deployed in a way that minimises and mitigates threats to their security. | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |
| 7. Secure development | Cloud services should be designed, developed and deployed in a way that minimises and mitigates threats to their security. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7. Secure developme nt | Cloud services should be designed, developed and deployed in a way that minimises and mitigates threats to their security. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | account-part-of-or ganizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsist ent account configura tions, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 9. Secure user management | Providers should make tools available to securely manage your use of their service. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individuals. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individuals. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individuals. | rds-instance-iam-authentication-enabled | Ensure an AWS Identity and Access Management (IAM) authentication is enabled on Amazon Relational Database Service (Amazon RDS) instances to control access to systems and assets. This enforces network traffic to and from the database to be encrypted using Secure Sockets Layer (SSL). You are not required to store user credentials in the database, as authentication is managed externally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individuals. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individua ls. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individua ls. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individua ls. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individuals. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individuals. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10. Identity and authentication | Access to service interfaces should be constrained to authenticated and authorised individuals. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | ecs-container-insights-enabled | Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Elastic Container Service (ECS) and your AWS solutions. Container Insights also provides diagnostic information, such as container restart failures, to help you isolate issues and resolve them quickly. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11. External interface protection | All external or less trusted interfaces to the service should be identified and defended. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12. Secure service administration | Cloud providers should recognise the high value of administration systems. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13. Audit information for users | Providers should supply logs needed to monitor access to your service, and the data held within it. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 13. Audit information for users | Providers should supply logs needed to monitor access to your service, and the data held within it. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13. Audit information for users | Providers should supply logs needed to monitor access to your service, and the data held within it. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 13. Audit information for users | Providers should supply logs needed to monitor access to your service, and the data held within it. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |

### Template

The template is available on GitHub: Operational Best Practices for NCSC Cloud Security Principles.

## Operational Best Practices for NCSC Cyber Assesment Framework

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) controls and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more UK NCSC CAF controls. A UK NCSC CAF control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This sample conformance pack template contains mappings to controls within the UK NCSC CAF (National Cyber Security Centre | NCSC CAF guidance), with such public sector information licensed under the Open Government Licence v3.0. The Open Government Licence should can be accessed here: Open Government Licence for public sector information.

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A3.a#Asset Management | Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling). | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |
| A3.a#Asset Management | Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling). | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |
| A3.a#Asset Management | Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling). | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.a#Asset Management | Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling). | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |
| A3.a#Asset Management | Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling). | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a#Identity Verification, Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.a Identity Verification,Authentication and Authorisation | You robustly verify,#authenticate and authorise access to the networks and information systems supporting your essential function. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| B2.b Device Management | You fully know and have trust in the devices that are used to access your networks, informati on systems and data that support your essential function. | ec2-instance-manag ed-by-systems-mana ger | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.b Device Management | You fully know and have trust in the devices that are used to access your networks, informati on systems and data that support your essential function. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | ecs-containers-non privileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitio ns should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | ecs-containers-rea donly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance' s filesystem cannot be modified unless it has explicit read-writ e permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.c Privileged User Management | You closely manage privileged user access to networks and information systems supporting the essential function. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d#Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good management and maintenance of identity and access control for your networks and information systems supporting the essential function. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B2.d Identity and Access Management (IdAM) | You assure good managemen t and maintenan ce of identity and access control for your networks and information systems supporting the essential function. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.a Understanding Data | You have a good understanding of data important to the operation of the essential function, where it is stored, where it travels and how unavailability or unauthorised access, modificat ion or deletion would adversely impact the essential function.# also applies to third parties storing or accessing data important to the operation of essential functions. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B3.b Data in Transit | You have protected the transit of data important to the operation of the essential function.#This includes the transfer of data to third parties. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| B3.c Stored Data | You have protected#stored data important to the operation of the essential function. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | alb-http-drop-inva lid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | internet-gateway-a uthorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | dynamodb-autoscali ng-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/writ e capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | dynamodb-throughput-limit-check | Enable this rule to ensure that provision ed throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionall y set accountRC UThresholdPercenta ge (Config Default: 80) and accountWC UThresholdPercenta ge (Config Default: 80) parameters. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | lambda-concurrency-check | This rule ensures that a Lambda function' s concurrency high and low limits are established. This can assist in baselinin g the number of requests that your function is serving at any given time. |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | ec2-instance-manag ed-by-systems-mana ger | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.a Secure by Design | You#design security into the network and informati on systems that support the operation c essential functions .#You minimise their attack surface and ensure that the operation of the essential function shoul not be impacted by the exploitation of any single vulnerabi lity. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.b Secure Configuration | You securely configure the#network and information systems that support the operation of essential functions. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B4.b Secure Configuration | You securely configure the#network and information systems that support the operation of essential functions. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| B4.b Secure Configuration | You securely configure the#network and information systems that support the operation of essential functions. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.b Secure Configuration | You securely configure the#network and information systems that support the operation of essential functions. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.c#Secure Management | You#manage#your organisat ion's#network and information systems that support the operation of essential functions to enable and maintain security. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |
| B4.c#Secure Management | You#manage#your organisat ion's#network and information systems that support the operation of essential functions to enable and maintain security. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.c#Secure Management | You#manage#your organisat ion's#network and information systems that support the operation of essential functions to enable and maintain security. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.d. Vulnerability Management | You#manage known vulnerabi lities in#your#network and informati on systems to prevent adverse impact on the essential functio | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associati ons to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configura tion state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configura tions, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.d. Vulnerability Management | You#manage known vulnerabi lities in#your#network and informati on systems to prevent adverse impact on the essential functio | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |
| B4.d. Vulnerability Management | You#manage known vulnerabi lities in#your#network and informati on systems to prevent adverse impact on the essential functio | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.d. Vulnerability Management | You#manage known vulnerabi lities in#your#network and informati on systems to prevent adverse impact on the essential functio | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.d. Vulnerability Management | You#manage known vulnerabi lities in#your#network and informati on systems to prevent adverse impact on the essential functio | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B4.d. Vulnerability Management | You#manage known vulnerabi lities in#your#network and informati on systems to prevent adverse impact on the essential functio | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.b Design for Resilience | You#design#the#netwc and information systems supportin g#your#essential functi be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.b Design for Resilience | You#design#the#netwc and information systems supportin g#your#essential functi be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.b Design for Resilience | You#design#the#netwc and information systems supportin g#your#essential functi be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| B5.c Backups | You hold accessible and secured current backups of data and information needed to recover operation of your essential function | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.a Monitoring Coverage | The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.b Securing Logs | You hold logging data securely and grant read access only to accounts with business need. No employee should ever need to#modify or delete logging data within an agreed retention period, after which it should be deleted. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.c Generating Alerts | Evidence of potential security incidents contained in your monitoring data is reliably identified and#triggers alerts. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.d Identifying Security Incidents | You contextua lise alerts with knowledge of the threat and your#systems, to identify those security incidents that require some form of response. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.d Identifying Security Incidents | You contextua lise alerts with knowledge of the threat and your#systems, to identify those security incidents that require some form of response. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.e Monitoring Tools and Skills | Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential functions they need to protect. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.e Monitoring Tools and Skills | Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential functions they need to protect. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C1.e Monitoring Tools and Skills | Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the essential functions they need to protect. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C2.a System Abnormalities for Attack Detection | You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| C2.a System Abnormalities for Attack Detection | You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| D1.c Testing and Exercising | Your#organizat ion carries out exercises to test response plans, using past incidents that affected your (and other) organizat ion, and scenarios that draw on threat intelligence and your risk assessment. | response-plan-exists-maintained (Process Check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel . Having updated and formally documente d response plans can assist in making sure response personnel understand roles, responsibilities and processes to be followed during an incident. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| D1.c Testing and Exercising | Your#organization carries out exercises to test response plans, using past incidents that affected your (and other) organization, and scenarios that draw on threat intelligence and your risk assessment. | response-plan-tested (Process Check) | Ensure Incident response and recovery plans are tested. This can assist in understanding if your plan will be effective during an incident and if any gaps or updates need to be addressed. |

### Template

The template is available on GitHub: Operational Best Practices for NCSC Cyber Assesment Framework.

## Operational Best Practices for Networking and Content Delivery Services

This conformance pack contains AWS Config rules based on Networking and Content Delivery Services. For more information, see Networking and Content Delivery on AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Networking and Content Delivery Services.

## Operational Best Practices for NIST 800-53 rev 4

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard.

You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST 800-53 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NIST 800-53 controls. A NIST 800-53 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

This Conformance Pack was validated by AWS Security Assurance Services LLC (AWS SAS), which is a team of Payment Card Industry Qualified Security Assessors (QSAs), HITRUST Certified Common Security Framework Practitioners (CCSFPs), and compliance professionals certified to provide guidance and assessments for various industry frameworks. AWS SAS professionals designed this Conformance Pack to enable a customer to align to a subset of the NIST 800-53.

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundatio ns Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(1) | The organization employs automated mechanisms to support the management of information system accounts. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(3) | The information system automatic ally disables inactive accounts after [Assignment: organization-defined time period]. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | The information system automatic ally audits account creation, modificat ion, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(12)(a) | The organization: a. Monitors informati on system accounts for [Assignment: organization-defined atypical use]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(12)(a) | The organization: a. Monitors informati on system accounts for [Assignment: organization-defined atypical use]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundations Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(f) | The organization: f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(g) | The organization: g. Monitors the use of information system accounts. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]. | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundatio ns Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-2(j) | The organization: j. Reviews accounts for compliance with account managemen t requirements [Assignment: organization-defined frequency]. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC-3 | The information system enforces approved authoriza tions for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | s3-account-level-public-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within anAmazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | s3-account-level-public-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-4 | The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5c | The organization: c. Defines information system access authorizations to support separation of duties. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-5c | The organization: c. Defines informati on system access authorizations to support separation of duties. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-account-level-p ublic-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| AC-6 | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6 | The organizat ion employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(10) | The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(1) | The information system monitors and controls remote access methods. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17(1) | The information system monitors and controls remote access methods. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-17(2) | The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17(3) | The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-account-level-public-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21(b) | The organization: b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defin ed auditable events]; d. Determines that the following events are to be audited within the informati on system: [Assignme nt: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring ) auditing for each identified event]. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defin ed auditable events]; d. Determines that the following events are to be audited within the informati on system: [Assignme nt: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring ) auditing for each identified event]. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-2(a)(d) | The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event]. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | The information system generates audit records containing informati on that establish es what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1)(3) | (1) The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. (3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-7(1) | The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-7(1) | The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| AU-9 | The information system protects audit information and audit tools from unauthorized access, modification, and deletion. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9(2) | The informati on system backs up audit records [Assignment: organization-defin ed frequency] onto a physically different system or system component than the system or component being audited. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| AU-11 | The organization retains audit records for [Assignment: organization-defin ed time period consistent with records retention policy] to provide support for after-the -fact investigations of security incidents and to meet regulatory and organizational information retention requirements. | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12(a)(c) | The informati on system: a. Provides audit record generation capabilit y for the auditable events defined in AU-2 a. at [Assignme nt: organization-defined information system component s]; c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7(a)(b) | The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-2 | The organization develops, documents , and maintains under configuration control, a current baseline configuration of the information system. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-7(a) | The organization: a. Configures the information system to provide only essential capabilities. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(1) | The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3)(a) | The organization: a. Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organization: b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level informati on contained in the information system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives]. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level informati on contained in the information system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives]. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9(b) | The organizat ion: b. Conducts backups of system-level informati on contained in the information system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives]. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-9(b) | The organizat ion: b. Conducts backups of system-level informati on contained in the information system [Assignment: organization-defined frequency consisten t with recovery time and recovery point objectives]. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-autoscali ng-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/writ e capacity to handle sudden increases in traffic, without throttling. |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | elb-deletion-prote ction-enabled | This rule ensures that Elastic Load Balancing has deletion protectio n enabled. Use this feature to prevent your load balancer from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilienc e requirements. It uses two tunnels to help ensure connectiv ity in case one of the Site-to-Site VPN connections becomes unavailab le. To protect against a loss of connectiv ity, in case your customer gateway becomes unavailab le, you can set up a second Site-to-S ite VPN connectio n to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-10 | The organizat ion provides for the recovery and reconstitution of the information system to a known state after a disruptio n, compromise, or failure. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2 | The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundatio ns Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1)(11) | (1) The information system implements multifactor authentication for network access to privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(1)(11) | (1) The information system implements multifactor authentication for network access to privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1)(2)(11) | (1) The information system implements multifactor authentication for network access to privileged accounts. (2) The information system implements multifactor authentication for network access to non- privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(1)(2)(11) | (1) The information system implements multifactor authentication for network access to privileged accounts. (2) The information system implements multifactor authentication for network access to non- privileged accounts. (11) The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(1)(a)(d)(e) | The information system, for password-based authentication: a. Enforces minimum password complexit y of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requireme nts for each type]; d. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization- defined numbers for lifetime minimum, lifetime maximum]; e. Prohibits password reuse for [Assignme nt: organization-defin ed number] generatio ns. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundatio ns Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(4) | The organization employs automated tools to determine if password authentic ators are sufficien tly strong to satisfy [Assignment: organization-defined requirements]. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the Centers for Internet Security (CIS) AWS Foundatio ns Benchmark for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organization's policies. |
| IA-5(7) | The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | The organization employs automated mechanisms to support the incident handling process. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-6(1) | The organization employs automated mechanisms to assist in the reporting of security incidents. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-7(1) | The organization employs automated mechanisms to increase the availability of incident response-related information and support. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times], in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-5 | The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times], in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3(a) | The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-10 | The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel]. | | |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-2 | The information system separates user functionality (including user interface services) from information system management functionality. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-4 | The information system prevents unauthorized and unintended informati on transfer from shared system resources. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5 | The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or references to sources for such information] by employing [Assignment: organization-defined security safeguards]. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within anAmazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | internet-gateway-a uthorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | sagemaker-notebook -no-direct-internet- access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-bucket-policy-g rantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_gran tee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principal s, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | s3-account-level-p ublic-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | alb-http-drop-inva lid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | The informati on system: a. Monitors and controls communications at the external boundary of the system and at key internal boundarie s within the system; b. Implements subnetworks for publicly accessible system component s that are [Selection: physically; logically ] separated from internal organizat ional networks; and c. Connects to external networks or information systems only through managed interface s consisting of boundary protectio n devices arranged in accordance with an organizational security architecture. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within anAmazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | The organization limits the number of external network connections to the information system. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-account-level-public-access-blocks | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(3) | The organization limits the number of external network connections to the information system. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | The organization limits the number of external network connections to the information system. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | The information system protects the [Selection (one or more): confident iality; integrity] of transmitted informati on. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-8(1) | The information system implement s cryptographic mechanisms to [Selection (one or more): prevent unauthori zed disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-8(1) | The information system implement s cryptographic mechanisms to [Selection (one or more): prevent unauthori zed disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | The information system implement s cryptographic mechanisms to [Selection (one or more): prevent unauthori zed disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-12 | The organization establishes and manages cryptogra phic keys for required cryptography employed within the information system in accordanc e with [Assignment: organization-defined requirements for key generation, distribut ion, storage, access, and destruction]. | cmk-backing-key-ro tation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| SC-12 | The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SC-13 | The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | The information system implements FIPS-validated or NSA-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| SC-23 | The information system protects the authenticity of communications sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | The information system protects the authenticity of communications sessions. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | The information system protects the authenticity of communications sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the [Selection (one or more): confident iality; integrity] of [Assignment: organization-defined information at rest]. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the [Selection (one or more): confident iality; integrity] of [Assignment: organization-defined information at rest]. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SC-28 | The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-36 | The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-36 | The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations. | rds-cluster-multi-az-enabled | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-36 | The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| SI-2(2) | The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-2(2) | The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(1) | The organizat ion connects and configures individua l intrusion detection tools into an information system-wide intrusion detection system. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-4(2) | The organization employs automated tools to support near real-time analysis of events. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-4(5) | The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization- defined compromise indicators]. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | The informati on system alerts [Assignment: organization-defin ed personnel or roles] when the following indicatio ns of compromise or potential compromis e occur: [Assignment: organization- defined compromise indicator s]. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(16) | The organization correlates informati on from monitorin g tools employed throughout the information system. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-4(a)(b)(c) | The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization- defined techniques and methods]; c. Deploys monitoring devices: i. strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7 | The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information]. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization- defined frequency]]. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization- defined frequency]]. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defin ed transitional states or security-relevant events]; [Assignment: organization- defined frequency]]. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organizat ion handles and retains information within the informati on system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulatio ns, standards, and operational requirements. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

### Template

The template is available on GitHub: Operational Best Practices for NIST 800-53 rev 4.

## Operational Best Practices for NIST 800-53 rev 5

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST 800-53 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NIST 800-53 controls. A NIST 800-53 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | Account Management \| Automated Audit Actions | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AC-2(4) | Account Management \| Automated Audit Actions | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| AC-2(4) | Account Management \| Automated Audit Actions | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AC-2(4) | Account Management \| Automated Audit Actions | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | Account Management \| Automated Audit Actions | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-2(4) | Account Management \| Automated Audit Actions | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | Account Managemen t \| Automated Audit Actions | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | Account Management \| Automated Audit Actions | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(4) | Account Management \| Automated Audit Actions | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2(12) | Account Management \| Account Monitoring for Atypical Usage | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| AC-2 | Account Management | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | Account Management | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | Account Management | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | Account Management | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | Account Management | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | Account Management | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-2 | Account Management | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| AC-3(15) | Access Enforcement \| Discretionary and Mandatory Access Control | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| AC-3 | Access Enforcement | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| AC-3 | Access Enforcement | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | Access Enforcement | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| AC-3 | Access Enforcement | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-3 | Access Enforcement | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| AC-3 | Access Enforcement | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | Access Enforcement | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | Access Enforcement | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-3 | Access Enforcement | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | Access Enforcement | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-3 | Access Enforcement | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-3 | Access Enforcement | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-3 | Access Enforcement | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-3 | Access Enforcement | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-4(26) | Information Flow Enforcement \| Audit Filtering Actions | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AC-5 | Separation of Duties | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5 | Separation of Duties | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| AC-5 | Separation of Duties | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5 | Separation of Duties | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-5 | Separation of Duties | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-5 | Separation of Duties | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-6(2) | Least Privilege \| Non-privileged Access for Nonsecurity Functions | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(2) | Least Privilege \| Non-privileged Access for Nonsecurity Functions | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6(2) | Least Privilege \| Non-privileged Access for Nonsecurity Functions | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(3) | Least Privilege \| Network Access to Privileged Commands | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| AC-6(3) | Least Privilege \| Network Access to Privileged Commands | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(3) | Least Privilege \| Network Access to Privileged Commands | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(3) | Least Privilege \| Network Access to Privileged Commands | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(3) | Least Privilege \| Network Access to Privileged Commands | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6(3) | Least Privilege \| Network Access to Privileged Commands | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-6(9) | Least Privilege \| Log Use of Privileged Functions | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6(10) | Least Privilege \| Prohibit Non-privileged Users from Executing Privileged Functions | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| AC-6(10) | Least Privilege \| Prohibit Non-privileged Users from Executing Privileged Functions | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-6(10) | Least Privilege \| Prohibit Non-privileged Users from Executing Privileged Functions | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| AC-17(2) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-17(2) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-17(2) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| AC-17(2) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17(2) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| AC-17(2) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-17(2) | Remote Access \| Protection of Confidentiality and Integrity Using Encryption | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| AC-21 | Information Sharing | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| AC-21 | Information Sharing | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| AC-21 | Information Sharing | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21 | Information Sharing | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| AC-21 | Information Sharing | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21 | Information Sharing | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| AC-21 | Information Sharing | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AC-21 | Information Sharing | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21 | Information Sharing | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| AC-21 | Information Sharing | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21 | Information Sharing | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| AC-21 | Information Sharing | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AC-21 | Information Sharing | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| AU-2 | Event Logging | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | Event Logging | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-2 | Event Logging | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AU-2 | Event Logging | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | Event Logging | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-2 | Event Logging | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | Event Logging | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-2 | Event Logging | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | Event Logging | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-2 | Event Logging | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | Event Logging | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | Event Logging | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-2 | Event Logging | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-3 | Content of Audit Records | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-3 | Content of Audit Records | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-3 | Content of Audit Records | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-3 | Content of Audit Records | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-3 | Content of Audit Records | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-3 | Content of Audit Records | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-6(1) | Audit Record Review, Analysis, and Reporting \| Automated Process Integration | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1) | Audit Record Review, Analysis, and Reporting \| Automated Process Integration | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1) | Audit Record Review, Analysis, and Reporting \| Automated Process Integration | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(1) | Audit Record Review, Analysis, and Reporting \| Automated Process Integration | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-6(3) | Audit Record Review, Analysis, and Reporting \| Correlate Audit Record Repositories | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(4) | Audit Record Review, Analysis, and Reporting \| Central Review and Analysis | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| AU-6(5) | Audit Record Review, Analysis, and Reporting \| Integrated Analysis of Audit Records | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(5) | Audit Record Review, Analysis, and Reporting \| Integrated Analysis of Audit Records | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(5) | Audit Record Review, Analysis, and Reporting \| Integrated Analysis of Audit Records | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-6(5) | Audit Record Review, Analysis, and Reporting \| Integrated Analysis of Audit Records | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-7(1) | Audit Record Reduction and Report Generation \| Automatic Processing | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-9(2) | Protection of Audit Information \| Store on Separate Physical Systems or Components | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-9(2) | Protection of Audit Information \| Store on Separate Physical Systems or Components | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| AU-9(2) | Protection of Audit Information \| Store on Separate Physical Systems or Components | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-9(7) | Protection of Audit Information \| Store on Component with Different Operating System | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-9 | Protection of Audit Information | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | Protection of Audit Information | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| AU-9 | Protection of Audit Information | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | Protection of Audit Information | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-9 | Protection of Audit Information | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| AU-10 | Non-repudiation | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-10 | Non-repudiation | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-10 | Non-repudiation | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| AU-10 | Non-repudiation | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-10 | Non-repudiation | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-10 | Non-repudiation | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| AU-10 | Non-repudiation | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-10 | Non-repudiation | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-10 | Non-repudiation | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-10 | Non-repudiation | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-10 | Non-repudiation | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-10 | Non-repudiation | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| AU-12 | Audit Record Generation | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| AU-12 | Audit Record Generation | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| AU-12 | Audit Record Generation | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-12 | Audit Record Generation | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| AU-14(1) | Session Audit \| System Start-up | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CA-7 | Continuous Monitoring | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitorin g | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |
| CA-7 | Continuous Monitorin g | s3-event-notificat ions-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modificat ions on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| CA-7 | Continuous Monitoring | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| CA-7 | Continuous Monitoring | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CA-7 | Continuous Monitoring | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| CA-7 | Continuous Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-7 | Continuous Monitoring | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| CA-9(1) | Internal System Connections \| Compliance Checks | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| CA-9(1) | Internal System Connections \| Compliance Checks | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| CA-9(1) | Internal System Connections \| Compliance Checks | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| CA-9(1) | Internal System Connections \| Compliance Checks | rds-instance-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Relational Database Service (Amazon RDS) database instance(s). |
| CA-9(1) | Internal System Connections \| Compliance Checks | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| CA-9(1) | Internal System Connections \| Compliance Checks | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| CA-9(1) | Internal System Connections \| Compliance Checks | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| CA-9(1) | Internal System Connections \| Compliance Checks | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CA-9(1) | Internal System Connections \| Compliance Checks | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CA-9(1) | Internal System Connections \| Compliance Checks | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CA-9(1) | Internal System Connections \| Compliance Checks | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| CA-9(1) | Internal System Connections \| Compliance Checks | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| CA-9(1) | Internal System Connections \| Compliance Checks | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| CA-9(1) | Internal System Connections \| Compliance Checks | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CA-9(1) | Internal System Connections \| Compliance Checks | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | redshift-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Redshift cluster(s). |
| CA-9(1) | Internal System Connections \| Compliance Checks | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| CA-9(1) | Internal System Connections \| Compliance Checks | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CA-9(1) | Internal System Connections \| Compliance Checks | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2(2) | Baseline Configuration \| Automation Support for Accuracy and Currency | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2(2) | Baseline Configuration \| Automation Support for Accuracy and Currency | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2(2) | Baseline Configuration \| Automation Support for Accuracy and Currency | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CM-2(2) | Baseline Configuration \| Automation Support for Accuracy and Currency | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2(2) | Baseline Configuration \| Automation Support for Accuracy and Currency | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-2(2) | Baseline Configura tion \| Automation Support for Accuracy and Currency | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-2 | Baseline Configuration | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| CM-2 | Baseline Configuration | rds-instance-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Relational Database Service (Amazon RDS) database instance(s). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | Baseline Configuration | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | Baseline Configuration | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | Baseline Configuration | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| CM-2 | Baseline Configuration | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | Baseline Configuration | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-2 | Baseline Configuration | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-2 | Baseline Configuration | redshift-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Redshift cluster(s). |
| CM-2 | Baseline Configuration | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-3(6) | Configuration Change Control \| Cryptography Management | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| CM-3(6) | Configuration Change Control \| Cryptography Management | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-3(6) | Configuration Change Control \| Cryptography Management | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-3(6) | Configuration Change Control \| Cryptography Management | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-3(6) | Configuration Change Control \| Cryptography Management | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| CM-3(6) | Configuration Change Control \| Cryptography Management | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-3(6) | Configuration Change Control \| Cryptography Management | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-3(6) | Configuration Change Control \| Cryptography Management | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-3(6) | Configuration Change Control \| Cryptography Management | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-3(6) | Configuration Change Control \| Cryptography Management | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| CM-3(6) | Configuration Change Control \| Cryptography Management | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-3 | Configuration Change Control | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| CM-3 | Configuration Change Control | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-7 | Least Functionality | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| CM-7 | Least Functionality | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-7 | Least Functionality | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(1) | System Component Inventory \| Updates During Installation and Removal | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(1) | System Component Inventory \| Updates During Installation and Removal | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(2) | System Component Inventory \| Automated Maintenance | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3) | System Component Inventory \| Automated Unauthorized Component Detection | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8(3) | System Component Inventory \| Automated Unauthorized Component Detection | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CM-8(3) | System Component Inventory \| Automated Unauthorized Component Detection | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| CM-8(3) | System Component Inventory \| Automated Unauthorized Component Detection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8 | System Component Inventory | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CM-8 | System Component Inventory | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-2(2) | Contingency Plan \| Capacity Planning | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-2(2) | Contingency Plan \| Capacity Planning | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-6(1) | Alternate Storage Site \| Separation from Primary Site | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6(2) | Alternate Storage Site \| Recovery Time and Recovery Point Objectives | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 | Alternate Storage Site | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 | Alternate Storage Site | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 | Alternate Storage Site | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 | Alternate Storage Site | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 | Alternate Storage Site | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-6 | Alternate Storage Site | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-6 | Alternate Storage Site | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-6 | Alternate Storage Site | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| CP-9 | System Backup | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| CP-9 | System Backup | dynamodb-pitr-enabled | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-9 | System Backup | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-9 | System Backup | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-10 | System Recovery and Reconstitution | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| CP-10 | System Recovery and Reconstitution | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| CP-10 | System Recovery and Reconstitution | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CP-10 | System Recovery and Reconstitution | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| CP-10 | System Recovery and Reconstitution | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CP-10 | System Recovery and Reconstitution | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Privileged Accounts | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Privileged Accounts | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Privileged Accounts | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(1) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Privileged Accounts | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA-2(2) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Non-privileged Accounts | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(2) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Non-privileged Accounts | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(2) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Non-privileged Accounts | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| IA-2(2) | Identification and Authentication (organizational Users) \| Multi-factor Authentication to Non-privileged Accounts | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA-2(6) | Identification and Authentication (organizational Users) \| Access to Accounts—separate Device | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(6) | Identification and Authentication (organizational Users) \| Access to Accounts —separate Device | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(6) | Identification and Authentication (organizational Users) \| Access to Accounts —separate Device | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(6) | Identification and Authentication (organizational Users) \| Access to Accounts —separate Device | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA-2(8) | Identification and Authentication (organizational Users) \| Access to Accounts — Replay Resistant | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(8) | Identification and Authentication (organizational Users) \| Access to Accounts — Replay Resistant | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(8) | Identification and Authentication (organizational Users) \| Access to Accounts — Replay Resistant | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-2(8) | Identification and Authentication (organizational Users) \| Access to Accounts — Replay Resistant | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| IA-5(1) | Authenticator Management \| Password-based Authentication | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(1) | Authenticator Management \| Password-based Authentication | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| IA-5(1) | Authenticator Management \| Password-based Authentication | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| IA-5(1) | Authenticator Management \| Password-based Authentication | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(1) | Authenticator Management \| Password-based Authentication | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| IA-5(1) | Authenticator Management \| Password-based Authentication | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(1) | Authenticator Management \| Password-based Authentication | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| IA-5(1) | Authenticator Management \| Password-based Authentication | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IA-5(7) | Authenticator Management \| No Embedded Unencrypted Static Authenticators | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(1) | Incident Handling \| Automated Incident Handling Processes | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| IR-4(5) | Incident Handling \| Automatic Disabling of System | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RA-3(4) | Risk Assessment \| Predictive Cyber Analytics | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SA-3 | System Development Life Cycle | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-3 | System Development Life Cycle | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SA-8(19) | Security and Privacy Engineering Principles \| Continuous Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SA-8(21) | Security and Privacy Engineering Principles \| Self-analysis | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SA-8(22) | Security and Privacy Engineering Principles \| Accountability and Traceability | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| SA-8(25) | Security and Privacy Engineering Principles \| Economic Security | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-11(1) | Developer Testing and Evaluation \| Static Code Analysis | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| SA-11(6) | Developer Testing and Evaluation \| Attack Surface Reviews | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-15(2) | Development Process, Standards, and Tools \| Security and Privacy Tracking Tools | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-15(2) | Development Process, Standards, and Tools \| Security and Privacy Tracking Tools | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-15(8) | Development Process, Standards, and Tools \| Reuse of Threat and Vulnerability Information | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SA-15(8) | Development Process, Standards, and Tools \| Reuse of Threat and Vulnerability Information | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SC-5(1) | Denial-of-service Protection \| Restrict Ability to Attack Other Systems | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(2) | Denial-of-service Protection \| Capacity, Bandwidth, and Redundancy | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-5(3) | Denial-of-service Protection \| Detection and Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| SC-5 | Denial-of-service Protection | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | Boundary Protection \| Access Points | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-7(3) | Boundary Protection \| Access Points | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | Boundary Protection \| Access Points | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | Boundary Protection \| Access Points | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(3) | Boundary Protection \| Access Points | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | Boundary Protection \| Access Points | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(3) | Boundary Protection \| Access Points | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(3) | Boundary Protection \| Access Points | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7(3) | Boundary Protection \| Access Points | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(3) | Boundary Protection \| Access Points | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(3) | Boundary Protection \| Access Points | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(4) | Boundary Protection \| External Telecommunications Services | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(4) | Boundary Protection \| External Telecommunications Services | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommu nications Services | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(4) | Boundary Protection \| External Telecommunications Services | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(5) | Boundary Protection \| Deny by Default — Allow by Exception | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(5) | Boundary Protection \| Deny by Default — Allow by Exception | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(5) | Boundary Protection \| Deny by Default — Allow by Exception | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(5) | Boundary Protection \| Deny by Default — Allow by Exception | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| SC-7(9) | Boundary Protection \| Restrict Threatening Outgoing Communications Traffic | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | rds-snapshot-encry pted | Ensure that encryptio n is enabled for your Amazon Relationa l Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| SC-7(10) | Boundary Protection \| Prevent Exfiltration | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protectio n \| Restrict Incoming Communications Traffic | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protectio n \| Restrict Incoming Communications Traffic | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protectio n \| Restrict Incoming Communications Traffic | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(11) | Boundary Protection \| Restrict Incoming Communications Traffic | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(16) | Boundary Protection \| Prevent Discovery of System Components | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(21) | Boundary Protection \| Isolation of System Components | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(21) | Boundary Protection \| Isolation of System Components | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(21) | Boundary Protection \| Isolation of System Components | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(21) | Boundary Protection \| Isolation of System Components | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7(21) | Boundary Protection \| Isolation of System Components | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7(21) | Boundary Protection \| Isolation of System Components | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7(21) | Boundary Protection \| Isolation of System Components | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| SC-7 | Boundary Protection | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| SC-7 | Boundary Protection | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| SC-7 | Boundary Protection | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| SC-7 | Boundary Protection | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| SC-7 | Boundary Protection | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-7 | Boundary Protection | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| SC-7 | Boundary Protection | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| SC-7 | Boundary Protection | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| SC-7 | Boundary Protection | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-7 | Boundary Protection | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8(1) | Transmission Confidentiality and Integrity \| Cryptographic Protection | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8(2) | Transmission Confidentiality and Integrity \| Pre- and Post-transmission Handling | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | Transmission Confidentiality and Integrity | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | Transmission Confidentiality and Integrity | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | Transmission Confidentiality and Integrity | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | Transmission Confidentiality and Integrity | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | Transmission Confidentiality and Integrity | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | Transmission Confidentiality and Integrity | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | Transmission Confidentiality and Integrity | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| SC-8 | Transmission Confidentiality and Integrity | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-8 | Transmission Confidentiality and Integrity | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-8 | Transmission Confidentiality and Integrity | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-12(2) | Cryptographic Key Establishment and Management \| Symmetric Keys | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12(2) | Cryptographic Key Establishment and Management \| Symmetric Keys | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| SC-12(3) | Cryptographic Key Establishment and Management \| Asymmetric Keys | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12(3) | Cryptographic Key Establishment and Management \| Asymmetric Keys | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-12(3) | Cryptographic Key Establishment and Management \| Asymmetric Keys | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| SC-12(3) | Cryptographic Key Establishment and Management \| Asymmetric Keys | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12(3) | Cryptographic Key Establishment and Management \| Asymmetric Keys | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| SC-12(3) | Cryptographic Key Establishment and Management \| Asymmetric Keys | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12(3) | Cryptographic Key Establishment and Management \| Asymmetric Keys | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-12 | Cryptographic Key Establishment and Management | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-12 | Cryptographic Key Establishment and Management | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| SC-13 | Cryptographic Protection | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| SC-13 | Cryptographic Protection | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-13 | Cryptographic Protection | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-13 | Cryptographic Protection | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| SC-13 | Cryptographic Protection | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| SC-13 | Cryptographic Protection | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SC-13 | Cryptographic Protection | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SC-13 | Cryptographic Protection | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-13 | Cryptographic Protection | api-gw-cache-enabl ed-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC-13 | Cryptographic Protection | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SC-13 | Cryptographic Protection | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-13 | Cryptographic Protection | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-13 | Cryptographic Protection | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC-13 | Cryptographic Protection | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| SC-13 | Cryptographic Protection | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-13 | Cryptographic Protection | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| SC-13 | Cryptographic Protection | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-13 | Cryptographic Protection | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-13 | Cryptographic Protection | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23(3) | Session Authenticity \| Unique System-generated Session Identifiers | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23(5) | Session Authenticity \| Allowed Certificate Authorities | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23(5) | Session Authenticity \| Allowed Certificate Authorities | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-23 | Session Authenticity | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | Session Authenticity | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | Session Authenticity | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | Session Authenticity | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-23 | Session Authenticity | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | Session Authenticity | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| SC-23 | Session Authenticity | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | Session Authenticity | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SC-23 | Session Authenticity | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-23 | Session Authenticity | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-28(1) | Protection of Information at Rest \| Cryptographic Protection | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28(3) | Protection of Information at Rest \| Cryptographic Keys | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| SC-28(3) | Protection of Information at Rest \| Cryptographic Keys | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |
| SC-28 | Protection of Information at Rest | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| SC-28 | Protection of Information at Rest | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| SC-28 | Protection of Information at Rest | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SC-28 | Protection of Information at Rest | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SC-28 | Protection of Information at Rest | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SC-28 | Protection of Information at Rest | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SC-28 | Protection of Information at Rest | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SC-28 | Protection of Information at Rest | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SC-28 | Protection of Information at Rest | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| SC-28 | Protection of Information at Rest | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SC-28 | Protection of Information at Rest | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-28 | Protection of Information at Rest | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| SC-28 | Protection of Information at Rest | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-36(2) | Distributed Processing and Storage \| Synchronization | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| SC-36 | Distributed Processing and Storage | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-36 | Distributed Processing and Storage | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SC-36 | Distributed Processing and Storage | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SC-36 | Distributed Processing and Storage | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | Flaw Remediation \| Automated Flaw Remediation Status | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SI-2(2) | Flaw Remediation \| Automated Flaw Remediation Status | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(2) | Flaw Remediation \| Automated Flaw Remediation Status | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(3) | Flaw Remediation \| Time to Remediate Flaws and Benchmarks for Corrective Actions | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(3) | Flaw Remediation \| Time to Remediate Flaws and Benchmarks for Corrective Actions | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(3) | Flaw Remediation \| Time to Remediate Flaws and Benchmarks for Corrective Actions | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SI-2(4) | Flaw Remediation \| Automated Patch Management Tools | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(4) | Flaw Remediation \| Automated Patch Management Tools | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(4) | Flaw Remediation \| Automated Patch Management Tools | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(5) | Flaw Remediation \| Automatic Software and Firmware Updates | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SI-2(5) | Flaw Remediation \| Automatic Software and Firmware Updates | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2(5) | Flaw Remediation \| Automatic Software and Firmware Updates | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | Flaw Remediation | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | Flaw Remediation | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | Flaw Remediation | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | Flaw Remediation | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-2 | Flaw Remediation | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | Flaw Remediation | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-2 | Flaw Remediation | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| SI-2 | Flaw Remediation | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-2 | Flaw Remediation | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-3(8) | Malicious Code Protection \| Detect Unauthorized Commands | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(1) | System Monitoring \| System-wide Intrusion Detection System | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SI-4(2) | System Monitoring \| Automated Tools and Mechanisms for Real-time Analysis | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(4) | System Monitoring \| Inbound and Outbound Communications Traffic | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |
| SI-4(4) | System Monitoring \| Inbound and Outbound Communications Traffic | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | System Monitoring \| System-generated Alerts | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(5) | System Monitoring \| System-generated Alerts | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-4(5) | System Monitoring \| System-generated Alerts | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(12) | System Monitoring \| Automated Organization-generated Alerts | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(13) | System Monitoring \| Analyze Traffic and Event Patterns | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| SI-4(20) | System Monitoring \| Privileged Users | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(20) | System Monitoring \| Privileged Users | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-4(20) | System Monitoring \| Privileged Users | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| SI-4(20) | System Monitoring \| Privileged Users | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(20) | System Monitoring \| Privileged Users | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| SI-4(20) | System Monitoring \| Privileged Users | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(20) | System Monitoring \| Privileged Users | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(20) | System Monitoring \| Privileged Users | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(20) | System Monitoring \| Privileged Users | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4(22) | System Monitoring \| Unauthorized Network Services | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| SI-4(25) | System Monitoring \| Optimize Network Traffic Analysis | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | System Monitoring | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | System Monitoring | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-4 | System Monitoring | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(1) | Software, Firmware, and Information Integrity \| Integrity Checks | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(3) | Software, Firmware, and Information Integrity \| Centrally Managed Integrity Tools | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(6) | Software, Firmware, and Information Integrity \| Cryptographic Protection | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(7) | Software, Firmware, and Information Integrity \| Integration of Detection and Response | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-7(8) | Software, Firmware, and Information Integrity \| Auditing Capability for Significant Events | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | Information Management and Retention | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | Information Management and Retention | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| SI-12 | Information Management and Retention | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | Information Management and Retention | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | Information Management and Retention | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | Information Management and Retention | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-12 | Information Management and Retention | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | s3-version-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| SI-13(5) | Predictable Failure Prevention \| Failover Capability | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-20 | Tainting | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| SI-20 | Tainting | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| SI-20 | Tainting | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

### Template

The template is available on GitHub: Operational Best Practices for NIST 800-53 rev 5.

## Operational Best Practices for NIST 800 171

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates,

are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST 800-171 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NIST 800-171 controls. A NIST 800-171 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.1 | Limit system access to authorized users, processes acting on behalf of authorize d users, and devices (including other systems). | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.2 | Limit system access to the types of transactions and functions that authorized users are permitted to execute. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.1.3 | Control the flow of CUI in accordance with approved authorizations. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3 | Control the flow of CUI in accordanc e with approved authorizations. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.4 | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.5 | Employ the principle of least privilege, including for specific security functions and privileged accounts. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.6 | Use non-privileged accounts or roles when accessing nonsecurity functions . | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.1.7 | Prevent non-privi leged users from executing privileged functions and audit the execution of such functions. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.7 | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.1.7 | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.7 | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.7 | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.1.7 | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.7 | Prevent non-privileged users from executing privileged functions and audit the execution of such functions. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| 3.1.12 | Monitor and control remote access sessions. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.12 | Monitor and control remote access sessions. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.12 | Monitor and control remote access sessions. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.12 | Monitor and control remote access sessions. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.12 | Monitor and control remote access sessions. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| 3.1.12 | Monitor and control remote access sessions. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.12 | Monitor and control remote access sessions. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 3.1.12 | Monitor and control remote access sessions. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.12 | Monitor and control remote access sessions. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| 3.1.12 | Monitor and control remote access sessions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.12 | Monitor and control remote access sessions. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.12 | Monitor and control remote access sessions. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.12 | Monitor and control remote access sessions. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.13 | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.14 | Route remote access from managed access control points. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 3.1.14 | Route remote access from managed access control points. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.1.14 | Route remote access from managed access control points. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.14 | Route remote access from managed access control points. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 3.1.14 | Route remote access from managed access control points. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 3.1.14 | Route remote access from managed access control points. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3.1.14 | Route remote access from managed access control points. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.14 | Route remote access from managed access control points. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.1.14 | Route remote access from managed access control points. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.14 | Route remote access from managed access control points. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.20 | Verify and control/limit connections to and use of external systems. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.20 | Verify and control/limit connections to and use of external systems. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.20 | Verify and control/limit connections to and use of external systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investiga tion, and reporting of unlawful, unauthori zed, or inappropriate system activity. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1 | Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Ensure that the actions of individua l system users can be uniquely traced to those users so they can be held accountable for their actions. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Ensure that the actions of individua l system users can be uniquely traced to those users so they can be held accountable for their actions. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.4 | Alert in the event of an audit process failure. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.4 | Alert in the event of an audit process failure. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.5 | Correlate audit review, analysis, and reporting processes for investigation and response to indicatio ns of inappropriate, suspicious, or unusual activity. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.5 | Correlate audit review, analysis, and reporting processes for investigation and response to indicatio ns of inappropriate, suspicious, or unusual activity. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.3.8 | Protect audit information and audit tools from unauthori zed access, modificat ion, and deletion. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.8 | Protect audit information and audit tools from unauthorized access, modification, and deletion. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |
| 3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.1 | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-instance-manag ed-by-systems-mana ger | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-managedinstanc e-association-comp liance-status-check | Use AWS Systems Manager Associati ons to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configura tion state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configura tions, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | ec2-volume-inuse-c heck | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminate d. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | opensearch-access-control-enabled | Ensure fine-grai ned access control is enabled on your Amazon OpenSearc h Service domains. Fine-grained access control provides enhanced authoriza tion mechanisms to achieve least-pri vileged access to Amazon OpenSearc h Service domains. It allows for role-base d access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-ten ancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | s3-bucket-level-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.6 | Employ the principle of least functiona lity by configuri ng organizational systems to provide only essential capabilities. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.4.7 | Restrict, disable, and prevent the use of nonessent ial, functions, ports, protocols, or services. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.7 | Restrict, disable, and prevent the use of nonessent ial, functions, ports, protocols, or services. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.7 | Restrict, disable, and prevent the use of nonessent ial, functions, ports, protocols, or services. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.7 | Restrict, disable, and prevent the use of nonessent ial, functions, ports, protocols, or services. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.9 | Control and monitor user-installed software. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.9 | Control and monitor user-installed software. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.3 | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.5 | Prevent reuse of identifiers for a defined period. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.6 | Disable identifiers after a defined period of inactivity. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.7 | Enforce a minimum password complexit y and change of characters when new passwords are created. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.8 | Prohibit password reuse for a specified number of generatio ns. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 3.5.10 | Store and transmit only cryptogra phically-protected passwords. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.10 | Store and transmit only cryptographically-protected passwords. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.5.10 | Store and transmit only cryptographically-protected passwords. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.5.10 | Store and transmit only cryptographically-protected passwords. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.10 | Store and transmit only cryptogra phically-protected passwords. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.5.10 | Store and transmit only cryptogra phically-protected passwords. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.10 | Store and transmit only cryptographically-protected passwords. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.10 | Store and transmit only cryptographically-protected passwords. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.10 | Store and transmit only cryptogra phically-protected passwords. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.5.10 | Store and transmit only cryptogra phically-protected passwords. | s3-bucket-server-s ide-encryption-ena bled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.10 | Store and transmit only cryptographically-protected passwords. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1 | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1 | Establish an operational incident-handling capabilit y for organizat ional systems that includes preparati on, detection, analysis, containme nt, recovery, and user response activities. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1 | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1 | Establish an operational incident-handling capabilit y for organizat ional systems that includes preparati on, detection, analysis, containme nt, recovery, and user response activities. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting the system are identified. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting the system are identified. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11.3 | Remediate vulnerabilities in accordance with assessments of risk. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communica tions (i.e., informati on transmitted or received by organizat ional systems) at the external boundaries and key internal boundarie s of organizational systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | autoscaling-launch -config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommend ed security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryptio n, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | sagemaker-notebook -no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.2 | Employ architectural designs, software development techniques, and systems engineeri ng principles that promote effective information security within organizational systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.6 | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.6 | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.6 | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.8 | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.13.10 | Establish and manage cryptographic keys for cryptography employed in organizational systems. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.10 | Establish and manage cryptographic keys for cryptography employed in organizational systems. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.16 | Protect the confidentiality of CUI at rest. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.16 | Protect the confidentiality of CUI at rest. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.16 | Protect the confidentiality of CUI at rest. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.16 | Protect the confidentiality of CUI at rest. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 3.13.16 | Protect the confidentiality of CUI at rest. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.16 | Protect the confidentiality of CUI at rest. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.16 | Protect the confidentiality of CUI at rest. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.16 | Protect the confidentiality of CUI at rest. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.16 | Protect the confidentiality of CUI at rest. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 3.13.16 | Protect the confidentiality of CUI at rest. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.1 | Identify, report, and correct information and system flaws in a timely manner. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.1 | Identify, report, and correct information and system flaws in a timely manner. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2 | Provide protection from malicious code at appropriate locations within organizational systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2 | Provide protection from malicious code at appropriate locations within organizational systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.3 | Monitor system security alerts and advisories and take actions in response. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.3 | Monitor system security alerts and advisories and take actions in response. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 3.14.3 | Monitor system security alerts and advisories and take actions in response. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.3 | Monitor system security alerts and advisories and take actions in response. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.3 | Monitor system security alerts and advisories and take actions in response. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.4 | Update malicious code protection mechanisms when new releases are available. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizat ional systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 3.14.7 | Identify unauthorized use of organizational systems. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| 3.14.7 | Identify unauthorized use of organizational systems. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 3.14.7 | Identify unauthorized use of organizational systems. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.14.7 | Identify unauthorized use of organizational systems. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| 3.14.7 | Identify unauthorized use of organizational systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7 | Identify unauthorized use of organizational systems. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.14.7 | Identify unauthorized use of organizational systems. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

### Template

The template is available on GitHub: Operational Best Practices for NIST 800 171.

## Operational Best Practices for NIST 800 172

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST 800-172 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NIST 800-172 controls. A NIST 800-172 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defin ed secure informati on transfer solutions ] to control informat ion flows between security domains on connected systems. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | alb-desync-mode-check | To assist in protecting applications for HTTP Desync vulnerabilities, ensure HTTP Desync mitigation mode is enabled on your application load balancers. HTTP Desync issues can lead to request smuggling and make your applications vulnerable to request queue or cache poisoning. Desync mitigation modes are monitor, defensive, and strictest. Defensive is the default mode. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | clb-desync-mode-check | To assist in protecting applications for HTTP Desync vulnerabilities, ensure HTTP Desync mitigation mode is enabled on your application load balancers. HTTP Desync issues can lead to request smuggling and make your applications vulnerable to request queue or cache poisoning. Desync mitigation modes are monitor, defensive, and strictest. Defensive is the default mode. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | ec2-token-hop-limit-check | Ensure the Instance Metadata Service (IMDS) HTTP PUT response is restricted to the Amazon Elastic Compute Cloud (Amazon EC2) instance. With IMDSv2, the PUT response that contains the secret token by default cannot travel outside the instance, because the Metadata response hop limit is set to 1 (Config default). If this value is greater than 1, the token is able to leave the EC2 instance. |
| 3.1.3e | Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems. | nacl-no-unrestricted-ssh-rdp | Access to remote server administration ports in your Network Access Control Lists (NACLs), such as port 22 (SSH) and port 3389 (RDP), should not be publicly accessible, as this may allow unintended access to resources within your VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.2.1e | Provide awareness training [Assignment: organization-defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization- defined frequency] or when there are significant changes to the threat. | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| 3.4.2e | Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.2e | Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.2e | Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.2e | Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4.3e | Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4.3e | Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| 3.4.3e | Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4.3e | Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| 3.4.3e | Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.2e | Employ automated mechanisms for the generation, protection, rotation, and managemen t of passwords for systems and system components that do not support multifact or authentication or complex account management. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 3.5.2e | Employ automated mechanisms for the generation, protection, rotation, and managemen t of passwords for systems and system components that do not support multifact or authentication or complex account management. | secretsmanager-rot ation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.2e | Employ automated mechanisms for the generation, protection, rotation, and managemen t of passwords for systems and system components that do not support multifact or authentication or complex account management. | secretsmanager-sch eduled-rotation-su ccess-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| 3.5.2e | Employ automated mechanisms for the generation, protection, rotation, and managemen t of passwords for systems and system components that do not support multifact or authentication or complex account management. | secretsmanager-sch eduled-rotation-su ccess-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.11.1e | Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.11.2e | Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.11.5e | Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence. | annual-risk-assessment-performed (process check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting an organization. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | nacl-no-unrestricted-ssh-rdp | Access to remote server administration ports in your Network Access Control Lists (NACLs), such as port 22 (SSH) and port 3389 (RDP), should not be publicly accessible, as this may allow unintended access to resources within your VPC. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.4e | Employ [Selectio n: (one or more): [Assignment: organization-defined physical isolation techniqu es]; [Assignment: organization-defin ed logical isolation techniques]] in organizational systems and system components. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.13.4e | Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.1e | Verify the integrity of [Assignment: organization-defined security critical or essential software] using root of trust mechanisms or cryptographic signatures. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2e | Monitor organizat ional systems and system components on an ongoing basis for anomalous or suspicious behavior. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.14.2e | Monitor organizat ional systems and system components on an ongoing basis for anomalous or suspicious behavior. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2e | Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2e | Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2e | Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2e | Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.2e | Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.6e | Use threat indicator information and effective mitigatio ns obtained from [Assignment: organization-defined external organizat ions] to guide and inform intrusion detection and threat hunting. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7e | Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques]. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7e | Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques]. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7e | Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques]. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7e | Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques]. | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatically for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.14.7e | Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques]. | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

### Template

The template is available on GitHub: Operational Best Practices for NIST 800 172.

## Operational Best Practices for NIST 800 181

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST 800 181 and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more NIST 800 181 controls. A NIST 800 181 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | and regulatory backup compliance requirements. |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| T0024 | Collect and maintain data needed to meet system cybersecurity reporting. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0042 | Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (for example, intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| T0047 | Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | backup-recovery-po int-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | dynamodb-autoscali ng-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/writ e capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | rds-instance-delet ion-protection-ena bled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropria te levels of system availability based on critical system functions and ensure that system requirements identify appropria te disaster recovery and continuity of operations requireme nts to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0051 | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| T0065 | Develop and implement network backup and recovery procedures. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0065 | Develop and implement network backup and recovery procedures. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| T0065 | Develop and implement network backup and recovery procedures. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0065 | Develop and implement network backup and recovery procedures. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| T0065 | Develop and implement network backup and recovery procedures. | dynamodb-pitr-enabled | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0065 | Develop and implement network backup and recovery procedures. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0065 | Develop and implement network backup and recovery procedures. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| T0065 | Develop and implement network backup and recovery procedures. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0086 | Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the managemen t authority for the intended operational environment. | rds-automatic-mino r-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed , which may include security patches and bug fixes. |
| T0086 | Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the managemen t authority for the intended operational environment. | ec2-managedinstanc e-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0086 | Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the managemen t authority for the intended operational environment. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environme nt ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0086 | Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the managemen t authority for the intended operational environment. | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0110 | Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0110 | Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0110 | Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| T0128 | Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0128 | Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| T0128 | Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0128 | Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0144 | Manage accounts, network rights, and access to systems and equipment. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0144 | Manage accounts, network rights, and access to systems and equipment. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0144 | Manage accounts, network rights, and access to systems and equipment. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0144 | Manage accounts, network rights, and access to systems and equipment. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0151 | Monitor and evaluate the effectiveness of the enterpris e's cybersecurity safeguards to ensure that they provide the intended level of protection. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0151 | Monitor and evaluate the effectiveness of the enterpris e's cybersecurity safeguards to ensure that they provide the intended level of protection. | cloudwatch-alarm-a ction-check | Amazon CloudWatc h alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequire d (Config Default: True), insuffici entDataActionRequi red (Config Default: True), okActionR equired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0151 | Monitor and evaluate the effectiveness of the enterpris e's cybersecurity safeguards to ensure that they provide the intended level of protection. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| T0152 | Monitor and maintain databases to ensure optimal performance. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| T0152 | Monitor and maintain databases to ensure optimal performance. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| T0152 | Monitor and maintain databases to ensure optimal performance. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| T0152 | Monitor and maintain databases to ensure optimal performance. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0152 | Monitor and maintain databases to ensure optimal performance. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0152 | Monitor and maintain databases to ensure optimal performance. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0153 | Monitor network capacity and performance. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0153 | Monitor network capacity and performance. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0153 | Monitor network capacity and performance. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0153 | Monitor network capacity and performance. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| T0156 | Oversee and make recommendations regarding configuration management. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configuration management. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configuration management. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configuration management. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configuration management. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configuration management. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configura tion management. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configura tion management. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0156 | Oversee and make recommendations regarding configura tion management. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0160 | Patch network vulnerabilities to ensure that informati on is safeguarded against outside parties. | rds-automatic-mino r-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed , which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0160 | Patch network vulnerabilities to ensure that informati on is safeguarded against outside parties. | ec2-managedinstanc e-association-comp liance-status-check | Use AWS Systems Manager Associati ons to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configura tion state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configura tions, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0160 | Patch network vulnerabilities to ensure that informati on is safeguarded against outside parties. | ec2-managedinstanc e-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | dynamodb-pitr-enabled | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0166 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0168 | Perform hash comparison against established database. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | autoscaling-launch -config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requireme nts. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0215 | Recognize a possible security violation and take appropriate action to report the incident, as required. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0244 | Verify that applicati on software/ network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrai l log file validation to check the integrity of CloudTrail logs. Log file validatio n helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithm s: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0244 | Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0244 | Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0258 | Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| T0259 | Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0262 | Employ approved defense-in-depth principles and practices (for example, defense-in-multiple places, layered defenses, security robustness). | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0284 | Design and develop new tools/tec hnologies as related to cybersecurity. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0306 | Supports incident managemen t, service-level management, change management, release managemen t, continuity management, and availability management for databases and data management systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0306 | Supports incident managemen t, service-level management, change management, release managemen t, continuity management, and availability management for databases and data management systems. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0306 | Supports incident managemen t, service-level management, change management, release managemen t, continuity management, and availability management for databases and data management systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0314 | Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0314 | Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0314 | Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| T0314 | Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0314 | Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0314 | Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecu rity requirements. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0333 | Perform cyber defense trend analysis and reporting. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0333 | Perform cyber defense trend analysis and reporting. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| T0347 | Assess the validity of source data and subsequent findings. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |
| T0358 | Design and develop system administration and managemen t functionality for privileged access users. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | multi-region-cloud trail-enabled | AWS CloudTrai l records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REG ION_CLOUD _TRAIL_ENABLED is enabled. Additiona lly, when AWS launches a new Region, CloudTrai l will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0376 | Establish, resource, implement , and assess cyber workforce managemen t programs in accordance with organizational requirements. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0416 | Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| T0416 | Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0416 | Enable applications with public keying by leveraging existing public key infrastru cture (PKI) libraries and incorpora ting certificate management and encryption functiona lities when appropria te. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0416 | Enable applications with public keying by leveraging existing public key infrastru cture (PKI) libraries and incorpora ting certificate management and encryption functiona lities when appropria te. | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0416 | Enable applications with public keying by leveraging existing public key infrastru cture (PKI) libraries and incorpora ting certificate management and encryption functiona lities when appropria te. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| T0416 | Enable applications with public keying by leveraging existing public key infrastru cture (PKI) libraries and incorpora ting certificate management and encryption functiona lities when appropria te. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0416 | Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0416 | Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0416 | Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0416 | Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0421 | Manage the indexing/ cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| T0421 | Manage the indexing/ cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (for example, hard copy documents, digital files). | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0491 | Install and configure hardware, software, and periphera l equipment for system users in accordance with organizational standards. | ec2-instance-manag ed-by-systems-mana ger | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0491 | Install and configure hardware, software, and periphera l equipment for system users in accordance with organizational standards. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0491 | Install and configure hardware, software, and periphera l equipment for system users in accordance with organizational standards. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |
| T0503 | Monitor external data sources (for example, cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0509 | Perform an informati on security risk assessment. | annual-risk-assess ment-performed (process check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determini ng the likelihood and impact of identified risks and/or vulnerabi lities affecting an organization. |
| T0553 | Apply cybersecu rity functions (for example, encryptio n, access control, and identity managemen t) to reduce exploitat ion opportunities. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon Elasticsearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elasticsearch Service (Amazon ES) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0553 | Apply cybersecurity functions (for example, encryption, access control, and identity management) to reduce exploitation opportunities. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| T0557 | Integrate key management functions as related to cyberspace. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated once they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0557 | Integrate key management functions as related to cyberspace. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| T0576 | Assess all-source intelligence and recommend targets to support cyber operation objectives. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0609 | Conduct access enabling of wireless computer and digital networks. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0609 | Conduct access enabling of wireless computer and digital networks. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| T0609 | Conduct access enabling of wireless computer and digital networks. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0609 | Conduct access enabling of wireless computer and digital networks. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon Elasticsearch Service (Amazon ES) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon ES domain within an Amazon VPC enables secure communication between Amazon ES and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0609 | Conduct access enabling of wireless computer and digital networks. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| T0616 | Conduct network scouting and vulnerability analyses of systems within a network. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0686 | Identify threat vulnerabilities. | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| T0686 | Identify threat vulnerabilities. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather information about networks through traditional and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| T0706 | Gather information about networks through traditional and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | elasticsearch-logs-to-cloudwatch | Ensure Amazon Elasticsearch service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | lambda-concurrency-check | This rule ensures that a Lambda function' s concurrency high and low limits are established. This can assist in baselinin g the number of requests that your function is serving at any given time. |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather information about networks through traditional and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | rds-enhanced-monit oring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availabil ity. This provides detailed visibility into the health of your Amazon RDS database instances . When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | beanstalk-enhanced -health-reporting- enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastru cture. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | cloud-trail-cloud- watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather information about networks through traditional and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | dynamodb-throughput-limit-check | Enable this rule to ensure that provision ed throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionall y set accountRC UThresholdPercenta ge (Config Default: 80) and accountWC UThresholdPercenta ge (Config Default: 80) parameters. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather information about networks through traditional and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| T0706 | Gather information about networks through traditional and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | redshift-cluster-c onfiguration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configura tions are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather informati on about networks through tradition al and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0706 | Gather information about networks through traditional and alternative techniques, (for example, social network analysis, call-chaining, traffic analysis.) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| T0777 | Profile network or system administrators and their activities. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0805 | Report intelligence-derived significant network events and intrusions. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| T0877 | Work cooperati vely with applicable organization units in overseeing consumer information access rights | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0877 | Work cooperati vely with applicable organization units in overseeing consumer information access rights | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0935 | Perform an informati on security risk assessment. | annual-risk-assess ment-performed (process check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determini ng the likelihood and impact of identified risks and/or vulnerabi lities affecting an organization. |
| T0960 | Monitor changes to a system and its environment of operation. | lambda-concurrency-check | This rule ensures that a Lambda function' s concurrency high and low limits are established. This can assist in baselinin g the number of requests that your function is serving at any given time. |
| T0960 | Monitor changes to a system and its environment of operation. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0960 | Monitor changes to a system and its environment of operation. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0960 | Monitor changes to a system and its environment of operation. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0960 | Monitor changes to a system and its environment of operation. | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0960 | Monitor changes to a system and its environment of operation. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0960 | Monitor changes to a system and its environment of operation. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0960 | Monitor changes to a system and its environment of operation. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitorin g results will be used in ongoing authoriza tion. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0992 | Determine how the continuous monitorin g results will be used in ongoing authoriza tion. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEnc ryptFrom). The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

### Template

The template is available on GitHub: Operational Best Practices for NIST 800 181.

## Operational Best Practices for NIST 1800 25

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between NIST 1800-25 and AWS managed Config rules. Each AWS Config applies to a specific AWS resource,and relates to one or more NIST 1800-25 controls. A NIST 1800-25 control can be related to multiple AWS Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-2 | Software platforms and applications within the organizat ion are inventoried | ec2-instance-manag ed-by-systems-mana ger | An inventory of the software platforms and applications within the organizat ion is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installat ions, application name, publisher and version, and other details about your environment. |
| ID.AM-2 | Software platforms and applications within the organizat ion are inventoried | ec2-managedinstanc e-association-comp liance-status-check | Use AWS Systems Manager Associati ons to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configura tion state to your |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | managed instances and allows you to set baselines of operating system patch levels, software installations, application configura tions, and other details about your environment. |
| ID.AM-2 | Software platforms and applications within the organizat ion are inventoried | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| ID.AM-2 | Software platforms and applications within the organizat ion are inventoried | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| ID.AM-2 | Software platforms and applications within the organizat ion are inventoried | vpc-network-acl-un used-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.RA-1 | Asset vulnerabilities are identified and documented | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| ID.RA-1 | Asset vulnerabilities are identified and documented | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| ID.RA-1 | Asset vulnerabilities are identified and documented | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| ID.RA-1 | Asset vulnerabilities are identified and documented | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorize d devices, users and processes | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorize d devices, users and processes | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorize d devices, users and processes | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |
| PR.AC-3 | Remote access is managed. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| PR.AC-3 | Remote access is managed. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.AC-3 | Remote access is managed. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.AC-3 | Remote access is managed. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-3 | Remote access is managed. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.AC-3 | Remote access is managed. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.AC-3 | Remote access is managed. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-3 | Remote access is managed. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| PR.AC-3 | Remote access is managed. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-3 | Remote access is managed. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | autoscaling-launch -config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | iam-policy-no-stat ements-with-full-a ccess | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| PR.DS-1 | Data-at-rest is protected | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| PR.DS-1 | Data-at-rest is protected | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-1 | Data-at-rest is protected | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| PR.DS-1 | Data-at-rest is protected | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| PR.DS-2 | Data-in-transit is protected | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| PR.DS-2 | Data-in-transit is protected | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-2 | Data-in-transit is protected | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| PR.DS-2 | Data-in-transit is protected | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| PR.DS-2 | Data-in-transit is protected | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| PR.IP-1 | A baseline configura tion of informati on technology/ industrial control systems is created and maintaine d incorporating security principles (for example concept of least functionality) | account-part-of-or ganizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsist ent account configura tions, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-3 | Configuration change control processes are in place | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| PR.IP-3 | Configuration change control processes are in place | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-9 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. | response-plan-exists-maintained (Process Check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel . Having updated and formally documente d response plans can assist in making sure response personnel understand roles, responsibilities and processes to be followed during an incident. |
| PR.IP-10 | Response and recovery plans are tested. | response-plan-tested (Process Check) | Ensure Incident response and recovery plans are tested. This can assist in understanding if your plan will be effective during an incident and if any gaps or updates need to be addressed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-12 | A vulnerability management plan is developed and implemented. | vuln-management-plan-exists (Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. This can include vulnerability management tools, environmental scanning cadence, roles and responsibilities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-12 | A vulnerability management plan is developed and implemented | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-12 | A vulnerability management plan is developed and implemented | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-12 | A vulnerability management plan is developed and implemented | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Communications and control networks are protected | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| PR.PT-4 | Communications and control networks are protected | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| PR.PT-4 | Communications and control networks are protected | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| PR.PT-4 | Communications and control networks are protected | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.PT-4 | Communications and control networks are protected | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PT-4 | Communications and control networks are protected | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.PT-4 | Communications and control networks are protected | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.PT-4 | Communications and control networks are protected | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.PT-4 | Communications and control networks are protected | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.PT-4 | Communications and control networks are protected | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| DE.CM-8 | Vulnerability scans are performed. | vuln-scans-performed (Process Check) | Ensure vulnerability scans are performed according to your compliance requirements. The cadence of scanning, tools used, and use of results should be defined by your organization. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks. | vuln-mitigated-accepted (Process Check) | Ensure newly identified vulnerabilities are remediated or documented as accepted risks. Services such as AWS Security Hub, Amazon Guard Duty, Amazon Inspector, and AWS Config can assist in identifying vulnerabilities within your environment. Vulnerabilities should be remediated or accepted as risks according to your organizations compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

### Template

The template is available on GitHub: Operational Best Practices for NIST 1800 25.

## Operational Best Practices for NIST CSF

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard.

You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST Cyber Security Framework (CSF) and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more NIST CSF controls. A NIST CSF control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-2 | Detected events are analyzed to understand attack targets and methods | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| DE.AE-2 | Detected events are analyzed to understand attack targets and methods | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environme nt. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains informati on such as the time the request was received, the client's IP address, latencies , request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-3 | Event data are collected and correlated from multiple sources and sensors | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| DE.AE-4 | Impact of events is determined | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-4 | Impact of events is determined | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| DE.AE-4 | Impact of events is determined | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| DE.AE-4 | Impact of events is determined | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-4 | Impact of events is determined | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-4 | Impact of events is determined | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-4 | Impact of events is determined | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.AE-4 | Impact of events is determined | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-1 | The network is monitored to detect potential cybersecu rity events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-1 | The network is monitored to detect potential cybersecu rity events | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-1 | The network is monitored to detect potential cybersecurity events | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecu rity events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-3 | Personnel activity is monitored to detect potential cybersecu rity events | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-4 | Malicious code is detected | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| DE.CM-4 | Malicious code is detected | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| DE.CM-5 | Unauthorized mobile code is detected | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-5 | Unauthorized mobile code is detected | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| DE.CM-5 | Unauthorized mobile code is detected | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-5 | Unauthorized mobile code is detected | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-5 | Unauthorized mobile code is detected | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-5 | Unauthorized mobile code is detected | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecu rity events | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecu rity events | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| DE.DP-4 | Event detection information is communicated | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.DP-4 | Event detection information is communicated | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| DE.DP-4 | Event detection information is communicated | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.DP-4 | Event detection information is communicated | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.DP-4 | Event detection information is communicated | s3-event-notifications-enabled | Amazon S3 event notifications can alert relevant personnel of any accidental or intentional modifications on your bucket objects. Example alerts include: new object is creation, object removal, object restoration, lost and replicated objects. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.DP-4 | Event detection information is communicated | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.DP-4 | Event detection information is communicated | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| DE.DP-5 | Detection processes are continuously improved | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-2 | Software platforms and applications within the organization are inventoried | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-2 | Software platforms and applications within the organization are inventoried | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-2 | Software platforms and applications within the organizat ion are inventoried | ec2-stopped-instance | Enable this rule to help with the baseline configura tion of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| ID.AM-2 | Software platforms and applications within the organizat ion are inventoried | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-2 | Software platforms and applications within the organization are inventoried | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |
| ID.AM-3 | Organizational communication and data flows are mapped | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-3 | Organizational communication and data flows are mapped | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-3 | Organizational communication and data flows are mapped | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-3 | Organizational communication and data flows are mapped | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-3 | Organizational communication and data flows are mapped | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-3 | Organizational communication and data flows are mapped | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.AM-3 | Organizational communication and data flows are mapped | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.BE-5 | Resilience requirements to support delivery of critical services are established for all operating states (for example under duress/attack, during recovery, normal operations) | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.RA-1 | Asset vulnerabilities are identified and documented | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| ID.RA-1 | Asset vulnerabilities are identified and documented | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| ID.RA-1 | Asset vulnerabilities are identified and documented | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |
| ID.RA-1 | Asset vulnerabilities are identified and documented | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.RA-2 | Cyber threat intelligence is received from information sharing forums and sources | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| ID.RA-3 | Threats, both internal and external, are identified and documented | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.RA-3 | Threats, both internal and external, are identified and documented | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| ID.SC-4 | Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.SC-4 | Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluatio ns to confirm they are meeting their contractual obligatio ns. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.SC-4 | Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.SC-4 | Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorize d devices, users and processes | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorize d devices, users and processes | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| PR.AC-3 | Remote access is managed. | autoscaling-launch -config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| PR.AC-3 | Remote access is managed. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.AC-3 | Remote access is managed. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.AC-3 | Remote access is managed. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.AC-3 | Remote access is managed. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.AC-3 | Remote access is managed. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-3 | Remote access is managed. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.AC-3 | Remote access is managed. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-3 | Remote access is managed. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.AC-4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-5 | Network integrity is protected (for example, network segregation, network segmentation) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-6 | Identities are proofed and bound to credentials and asserted in interactions | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-6 | Identities are proofed and bound to credentials and asserted in interacti ons | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-7 | Users, devices, and other assets are authenticated (for example, single-factor, multi-fac tor) commensur ate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| PR.AC-7 | Users, devices, and other assets are authenticated (for example, single-factor, multi-fac tor) commensur ate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks) | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-7 | Users, devices, and other assets are authenticated (for example, single-factor, multi-factor) commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks) | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-7 | Users, devices, and other assets are authenticated (for example, single-factor, multi-factor) commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-7 | Users, devices, and other assets are authenticated (for example, single-factor, multi-factor) commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| PR.AT-1 | All users are informed and trained | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-1 | Data-at-rest is protected | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| PR.DS-1 | Data-at-rest is protected | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| PR.DS-1 | Data-at-rest is protected | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| PR.DS-1 | Data-at-rest is protected | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-1 | Data-at-rest is protected | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| PR.DS-1 | Data-at-rest is protected | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| PR.DS-2 | Data-in-transit is protected | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| PR.DS-2 | Data-in-transit is protected | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| PR.DS-2 | Data-in-transit is protected | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| PR.DS-2 | Data-in-transit is protected | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-2 | Data-in-transit is protected | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-4 | Adequate capacity to ensure availability is maintained | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-4 | Adequate capacity to ensure availability is maintained | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.DS-5 | Protections against data leaks are implemented | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| PR.DS-5 | Protections against data leaks are implemented | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-5 | Protections against data leaks are implemented | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |
| PR.DS-5 | Protections against data leaks are implemented | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-5 | Protections against data leaks are implemented | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |
| PR.DS-5 | Protections against data leaks are implemented | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.DS-5 | Protections against data leaks are implemented | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.DS-5 | Protections against data leaks are implemented | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-5 | Protections against data leaks are implemented | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.DS-5 | Protections against data leaks are implemented | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-7 | The development and testing environme nt(s) are separate from the production environment | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (for example concept of least functionality) | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositories. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-3 | Configuration change control processes are in place | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| PR.IP-3 | Configuration change control processes are in place | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| PR.IP-4 | Backups of informati on are conducted , maintained, and tested | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-7 | Protection processes are improved | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| PR.IP-8 | Effectiveness of protection technologies is shared | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-8 | Effectiveness of protection technologies is shared | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.IP-8 | Effectiveness of protection technologies is shared | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-8 | Effectiveness of protection technologies is shared | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.IP-8 | Effectiveness of protection technologies is shared | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-8 | Effectiveness of protection technologies is shared | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.IP-8 | Effectiveness of protection technologies is shared | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-8 | Effectiveness of protection technologies is shared | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| PR.IP-8 | Effectiveness of protection technologies is shared | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-8 | Effectiveness of protection technologies is shared | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.IP-8 | Effectiveness of protection technologies is shared | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-8 | Effectiveness of protection technologies is shared | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-12 | A vulnerability management plan is developed and implemented | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-12 | A vulnerability management plan is developed and implemented | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.IP-12 | A vulnerability management plan is developed and implemented | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Communications and control networks are protected | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.PT-3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| PR.PT-4 | Communications and control networks are protected | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| PR.PT-4 | Communications and control networks are protected | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.PT-4 | Communications and control networks are protected | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.PT-4 | Communications and control networks are protected | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PT-4 | Communications and control networks are protected | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.PT-4 | Communications and control networks are protected | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.PT-4 | Communications and control networks are protected | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.PT-4 | Communications and control networks are protected | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-4 | Communications and control networks are protected | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-5 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RC.RP-1 | Recovery plan is executed during or after a cybersecurity incident | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.AN-2 | The impact of the incident is understood | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| RS.RP-1 | Response plan is executed during or after an incident | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| RS.RP-1 | Response plan is executed during or after an incident | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| RS.RP-1 | Response plan is executed during or after an incident | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| RS.RP-1 | Response plan is executed during or after an incident | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| RS.RP-1 | Response plan is executed during or after an incident | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| RS.RP-1 | Response plan is executed during or after an incident | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

### Template

The template is available on GitHub: Operational Best Practices for NIST CSF.

## Operational Best Practices for NIST Privacy Framework v1.0

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom

AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the NIST Privacy Framework and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more NIST Privacy Framework controls. A NIST Privacy Framework control can be related to multiple AWS Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P7 | Mechanisms for transmitting processing permissio ns and related data values with data elements are established and in place. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CT.DM-P7 | Mechanisms for transmitting processing permissio ns and related data values with data elements are established and in place. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P7 | Mechanisms for transmitting processing permissio ns and related data values with data elements are established and in place. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P7 | Mechanisms for transmitting processing permissio ns and related data values with data elements are established and in place. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CT.DM-P7 | Mechanisms for transmitting processing permissio ns and related data values with data elements are established and in place. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P7 | Mechanisms for transmitting processing permissions and related data values with data elements are established and in place. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| CT.DM-P7 | Mechanisms for transmitting processing permissions and related data values with data elements are established and in place. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| CT.DM-P7 | Mechanisms for transmitting processing permissions and related data values with data elements are established and in place. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| CT.DM-P7 | Mechanisms for transmitting processing permissions and related data values with data elements are established and in place. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | audit-log-policy-exists(Process Check) | Establish and maintain an audit log management policy that defines your organization's logging requirements. This includes, but is not limited to, review and retention of audit logs. |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy and incorpora ting the principle of data minimization. | dynamodb-throughput-limit-c heck | Enable this rule to ensure that provision ed throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughpu t requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionall y set accountRC UThresholdPercenta ge (Config Default: 80) and accountWC UThresholdPercenta ge (Config Default: 80) parameters. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy and incorpora ting the principle of data minimization. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy and incorpora ting the principle of data minimization. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy and incorpora ting the principle of data minimization. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy and incorpora ting the principle of data minimization. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy and incorpora ting the principle of data minimization. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| CT.DM-P8 | Audit/log records are determine d, documented, implemented, and reviewed in accordance with policy and incorpora ting the principle of data minimization. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearc h Service error logs can assist with security and access audits, and can help to diagnose availabil ity issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| CT.DM-P8 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| ID.DE-P2 | Data processing ecosystem parties (for example, service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. | annual-risk-assessment-performed(Process Check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting an organization. |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes , and devices. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes , and devices. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes , and devices. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes , and devices. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes , and devices. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes , and devices. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| PR.AC-P1 | Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes , and devices. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.AC-P3 | Remote access is managed. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| PR.AC-P3 | Remote access is managed. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| PR.AC-P3 | Remote access is managed. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-P3 | Remote access is managed. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.AC-P3 | Remote access is managed. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P3 | Remote access is managed. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| PR.AC-P3 | Remote access is managed. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | iam-policy-no-stat ements-with-admin-access | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissio ns and authoriza tions are managed, incorporating the principles of least privilege and separation of duties. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privileges it is because the customer has specifically opted-in to those configurations. This control checks for unexpected privilege escalation when a task definition has host networking enabled but the customer has not opted-in to elevated privileges. |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P4 | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P5 | Network integrity is protected (for example, network segregation, network segmentation). | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P6 | Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks). | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| PR.AC-P6 | Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks). | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P6 | Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks). | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P6 | Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks). | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.AC-P6 | Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (for example, individuals' security and privacy risks and other organizational risks). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| PR.DS-P1 | Data-at-rest are protected. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| PR.DS-P1 | Data-at-rest are protected. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| PR.DS-P1 | Data-at-rest are protected. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| PR.DS-P1 | Data-at-rest are protected. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| PR.DS-P1 | Data-at-rest are protected. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |
| PR.DS-P1 | Data-at-rest are protected. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |
| PR.DS-P1 | Data-at-rest are protected. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P1 | Data-at-rest are protected. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| PR.DS-P1 | Data-at-rest are protected. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-P1 | Data-at-rest are protected. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |
| PR.DS-P1 | Data-at-rest are protected. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-P1 | Data-at-rest are protected. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| PR.DS-P2 | Data-in-transit are protected. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-P2 | Data-in-transit are protected. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| PR.DS-P2 | Data-in-transit are protected. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| PR.DS-P2 | Data-in-transit are protected. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P2 | Data-in-transit are protected. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P4 | Adequate capacity to ensure availability is maintained. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| PR.DS-P5 | Protections against data leaks are implemented. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-P5 | Protections against data leaks are implemented. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| PR.DS-P5 | Protections against data leaks are implemented. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.DS-P5 | Protections against data leaks are implemented. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |
| PR.DS-P5 | Protections against data leaks are implemented. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.DS-P5 | Protections against data leaks are implemented. | vpc-flow-logs-enab led | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interface s in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| PR.DS-P5 | Protections against data leaks are implemented. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| PR.DS-P5 | Protections against data leaks are implemented. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.DS-P5 | Protections against data leaks are implemented. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.DS-P5 | Protections against data leaks are implemented. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.DS-P5 | Protections against data leaks are implemented. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| PR.DS-P6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.MA-P2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |
| PR.MA-P2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P1 | A baseline configuration of information technology is created and maintained incorporating security principles (for example, concept of least functionality). | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P1 | A baseline configuration of information technology is created and maintained incorporating security principles (for example, concept of least functionality). | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P1 | A baseline configuration of information technology is created and maintained incorporating security principles (for example, concept of least functionality). | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P1 | A baseline configuration of information technology is created and maintained incorporating security principles (for example, concept of least functionality). | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |
| PR.PO-P1 | A baseline configuration of information technology is created and maintained incorporating security principles (for example, concept of least functionality). | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P1 | A baseline configuration of information technology is created and maintained incorporating security principles (for example, concept of least functionality). | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P1 | A baseline configura tion of information technology is created and maintaine d incorporating security principles (for example, concept of least functiona lity). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PO-P1 | A baseline configuration of information technology is created and maintained incorporating security principles (for example, concept of least functionality). | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| AT-1: PR.PO-P10 | A vulnerability management plan is developed and implemented. | vuln-management-plan-exists(Process Check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P2 | Configuration change control processes are established and in place. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| PR.PO-P2 | Configuration change control processes are established and in place. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | dynamodb-in-backup -plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | dynamodb-pitr-enab led | Enable this rule to check that informati on has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | ebs-optimized-inst ance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/ O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contentio n between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | redshift-backup-en abled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | s3-bucket-replicat ion-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replicati on (CRR) supports maintaining adequate capacity and availabil ity. CRR enables automatic, asynchron ous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | aurora-resources-p rotected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | backup-plan-min-fr equency-and-min-re tention-check | To help with data back-up processes , ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) and requiredF requencyUnit (Config default: days) parameters. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | backup-recovery-po int-encrypted | Ensure that encryptio n is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | backup-recovery-po int-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | backup-recovery-po int-minimum-retent ion-check | To help with data back-up processes , ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. This rule allows you to set the requiredRetentionD ays (config default: 35) parameter. The actual value should reflect your organizat ions requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | ec2-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P3 | Backups of informati on are conducted , maintained, and tested. | fsx-resources-prot ected-by-backup-pl an | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PO-P7 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| PR.PO-P8 | Response and recovery plans are tested. | response-plan-tested(Process Check) | Ensure Incident response and recovery plans are tested. This can assist in understanding if your plan will be effective during an incident and if any gaps or updates need to be addressed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| PR.PT-P2 | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | redshift-enhanced-vpc-routing-enabled | Enhanced VPC routing forces all COPY and UNLOAD traffic between the cluster and data repositories to go through your Amazon VPC. You can then use VPC features such as security groups and network access control lists to secure network traffic. You can also use VPC flow logs to monitor network traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| PR.PT-P3 | Communications and control networks are protected. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| PR.PT-P3 | Communications and control networks are protected. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| PR.PT-P3 | Communications and control networks are protected. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| PR.PT-P3 | Communications and control networks are protected. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| PR.PT-P3 | Communications and control networks are protected. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| PR.PT-P3 | Communications and control networks are protected. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| PR.PT-P3 | Communications and control networks are protected. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| PR.PT-P3 | Communications and control networks are protected. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P3 | Communications and control networks are protected. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| PR.PT-P3 | Communications and control networks are protected. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| PR.PT-P4 | Mechanisms (for example, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

### Template

The template is available on GitHub: Operational Best Practices for NIST Privacy Framework v1.0.

## Operational Best Practices for NYDFS 23

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the New York State Department Of Financial Services (NYDFS) cybersecurity requirements for financial services companies (23 NYCRR 500) and

AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more US NYDFS controls. A US NYDFS 23 NYCRR 500 control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confident iality, integrity and availability of the Covered Entity's Information Systems. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confident iality, integrity and availability of the Covered Entity's Information Systems. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confident iality, integrity and availability of the Covered Entity's Information Systems. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confident iality, integrity and availability of the Covered Entity's Information Systems. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confident iality, integrity and availability of the Covered Entity's Information Systems. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(a) | (a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confident iality, integrity and availability of the Covered Entity's Information Systems. | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecu rity functions: (2) use defensive infrastructure and the implement ation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unau thorized access, use or other malicious acts. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecu rity functions: (2) use defensive infrastructure and the implement ation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unau thorized access, use or other malicious acts. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(2) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (3) detect Cybersecurity Events. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 500.02(b)(3) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (3) detect Cybersecurity Events. | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (3) detect Cybersecurity Events. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (3) detect Cybersecurity Events. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 500.02(b)(3) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (3) detect Cybersecurity Events. | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (3) detect Cybersecurity Events. | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(3) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (3) detect Cybersecurity Events. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.02(b)(5) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecu rity program shall be based on the Covered Entity's Risk Assessment and designed to perfor m the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.02(b)(5) | (b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions: (5) recover from Cybersecurity Events and restore normal operations and services. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventing accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.05 | The cybersecurity program for each covered entity shall include monitoring and testing, developed in accordance with the covered entity's risk assessment, designed to assess the effectiveness of the covered entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities, covered entities shall conduct: (a) annual penetration testing of the covered entity's information systems determined | vuln-management-plan-exists (process check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | each given year based on relevant identifie d risks in accordanc e with the risk assessment; and (b) bi-annual vulnerabi lity assessmen ts, including any systematic scans or reviews of informati on systems reasonabl y designed to identify publicly known cybersecu rity vulnerabilities in the covered entity's information systems based on the risk assessment. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(b) | (b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three yea rs. | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.06(a) | (a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment: (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearc h Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | ecs-task-definition-user-for-host-mode-check | If a task definition has elevated privilege s it is because the customer has specifically opted-in to those configura tions. This control checks for unexpecte d privilege escalation when a task definitio n has host networkin g enabled but the customer has not opted-in to elevated privileges. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | no-unrestricted-ro ute-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | s3-account-level-p ublic-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthori zed remote users by preventing public access. This rule allows you to optionally set the ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | ssm-document-not-p ublic | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | iam-user-unused-cr edentials-check | AWS Identity and Access Managemen t (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentia ls, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | secretsmanager-rot ation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potential ly reduce the business impact if the secret is compromised. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | secretsmanager-sch eduled-rotation-su ccess-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | emr-kerberos-enabl ed | The access permissio ns and authoriza tions can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribut ion center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | s3-bucket-policy-g rantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_gran tee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principal s, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | ec2-instance-no-pu blic-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearc h Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | emr-master-no-publ ic-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | internet-gateway-a uthorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | lambda-function-pu blic-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potential ly lead to degradati on of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | redshift-cluster-p ublic-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | s3-bucket-public-r ead-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | s3-bucket-public-w rite-prohibited | Manage access to resources in the AWS Cloud by only allowing authorize d users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 500.07 | As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Informati on and shall per iodically review such access privileges. | sagemaker-notebook -no-direct-internet- access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.8(a) | (a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment. | codebuild-project-envvar-awscred-check | Ensure authentication credentials AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY do not exist within AWS Codebuild project environments. Do not store these variables in clear text. Storing these variables in clear text leads to unintended data exposure and unauthorized access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.8(a) | (a) Each Covered Entity's cybersecurity program shall include written procedure s, guidelines and standards designed to ensure the use of secure developme nt practices for in-house developed applications utilized by the Covered Entity, and procedure s for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment. | codebuild-project-source-repo-url-check | Ensure the GitHub or Bitbucket source repository URL does not contain personal access tokens, sign-in credentials within AWS Codebuild project environments. Use OAuth instead of personal access tokens or sign-in credentials to grant authorization for accessing GitHub or Bitbucket repositor ies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.09 | (a) Each covered entity shall conduct a periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program as required by this Part. Such risk assessment shall be updated as reasonably necessary to address changes to the covered entity's information systems, nonpublic informati on or business operations. The covered entity's risk assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the covered entity's business operations related to cybersecu rity, nonpublic information collected | annual-risk-assess ment-performed (process check)> | Perform an annual risk assessment on your organization. Risk assessments can assist in determini ng the likelihood and impact of identified risks and/or vulnerabi lities affecting an organization. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | or stored, informati on systems utilized and the availability and effectiveness of controls to protect nonpublic informati on and information systems. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.12 | (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.12 | (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.12 | (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.12 | (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.12 | (a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | cloudwatch-alarm-action-check | Amazon CloudWatch alarms alert when a metric breaches the threshold for a specified number of evaluation periods. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. This rule requires a value for alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). The actual value should reflect the alarm actions for your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |
| 500.14(a) | (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.14(b) | As part of its cybersecurity program, each covered entity shall: (b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the covered entity in its risk assessment. | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Managemen t Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | s3-default-encrypt ion-kms | Ensure that encryptio n is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| 500.15(a) | (a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 500.16 | (a) As part of its cybersecurity program, each covered entity shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event materially affecting the confidentiality, integrity or availabil ity of the covered entity's informati on systems or the continuing functiona lity of any aspect of the covered entity's business or operation s. | response-plan-exists-maintained (process check) | Ensure incident response plans are established, maintained, and distributed to responsible personnel . |

### Template

The template is available on GitHub: Operational Best Practices for NYDFS 23.

## Operational Best Practices for NZISM 3.8

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the New Zealand Government Communications Security Bureau (GCSB) Information Security Manual (NZISM) 2022-09 Version 3.8 and AWS Managed Config rules. Each Config rule applies to a specific AWS resource type, and relates to one or more NZISM controls. An NZISM control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings. Only controls representing recommended or baseline practice for information classified RESTRICTED and below are included in the mappings.

This sample conformance pack template contains mappings to controls within the NZISM framework, which is an integral part of the Protective Security Requirements (PSR) framework that sets out the New Zealand Government's expectations for the management of personnel, information and physical security.

The NZISM is licensed under the Creative Commons Attribution 4.0 New Zealand licence, available at https://creativecommons.org/licenses/by/4.0/. Copyright information can be found at NZISM New Zealand Information Security Manual | Legal, Privacy, and Copyright.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1149 | Software security, Standard Operating Environments, Developing hardened SOEs (14.1.8.C.01.) | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | name, publisher and version, and other details about your environment. |
| 1149 | Software security, Standard Operating Environments, Developing hardened SOEs (14.1.8.C.01.) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1149 | Software security, Standard Operating Environments, Developing hardened SOEs (14.1.8.C.01.) | ecs-containers-non privileged | This control checks if the privileged parameter in the container definitio n of Amazon ECS Task Definitions is set to true. The control fails if this parameter is equal to true. This control only evaluates the latest active revision of an Amazon ECS task definition. We recommend that you remove elevated privileges from your ECS task definitions. When the privilege parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1149 | Software security, Standard Operating Environments, Developing hardened SOEs (14.1.8.C.01.) | ecs-containers-readonly-access | This control checks if Amazon ECS containers are limited to read-only access to mounted root filesystems. This control fails if the ReadonlyRootFilesystem parameter in the container definition of Amazon ECS task definitions is set to false. This control only evaluates the latest active revision of an Amazon ECS task definition. Enabling this option reduces security attack vectors since the container instance's filesystem cannot be tampered with or written to unless it has explicit read-write permissions on its filesystem folder and directories. This control also adheres to the principle of least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1661 | Software security, Web Application Development, Agency website content (14.5.6.C.01.) | cloudfront-default-root-object-configured | This control checks whether an Amazon CloudFront distribution is configured to return a specific object that is the default root object. The control fails if the CloudFront distribution does not have a default root object configured. A user might sometimes request the distribution's root URL instead of an object in the distribution. When this happens, specifying a default root object can help you to avoid exposing the contents of your web distribution. This rule must be applied in the us-east-1 region. Deploy with template parameter DeployEdgeRules = true |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1667 | Software security, Web Application Development, Web applications (14.5.8.C.01.) | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration. The value is 90 days. |
| 1667 | Software security, Web Application Development, Web applications (14.5.8.C.01.) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1841 | Access Control and Passwords, Identification, Authentication and Passwords, Methods for system user identification and authentication (16.1.35.C.02.) | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1841 | Access Control and Passwords, Identification, Authentication and Passwords, Methods for system user identification and authentication (16.1.35.C.02.) | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1841 | Access Control and Passwords, Identification, Authentication and Passwords, Methods for system user identification and authentication (16.1.35.C.02.) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1841 | Access Control and Passwords, Identification, Authentication and Passwords, Methods for system user identification and authentication (16.1.35.C.02.) | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 1847 | Access Control and Passwords, Identification, Authentication and Passwords, Protecting authentication data in transit (16.1.37.C.01.) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1847 | Access Control and Passwords, Identification, Authentication and Passwords, Protecting authentication data in transit (16.1.37.C.01.) | cloudfront-viewer-policy-https | This control checks whether an Amazon CloudFront distribution requires viewers to use HTTPS directly or whether it uses redirection. The control fails if ViewerProtocolPolicy is set to allow-all for defaultCacheBehavior or for cacheBehaviors. HTTPS (TLS) can be used to help prevent potential attackers from using person-in-the-middle or similar attacks to eavesdrop on or manipulate network traffic. Only encrypted connections over HTTPS (TLS) should be allowed. This rule must be applied in the us-east-1 region. Deploy with template parameter DeployEdgeRules = true |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1847 | Access Control and Passwords, Identification, Authentication and Passwords, Protecting authentication data in transit (16.1.37.C.01.) | elasticsearch-node-to-node-encryption-check | This control checks whether Elasticsearch domains have node-to-node encryption enabled. This control fails if node-to-node encryption is disabled on the domain. HTTPS (TLS) can be used to help prevent potential attackers from eavesdropping on or manipulating network traffic using person-in-the-middle or similar attacks. Only encrypted connections over HTTPS (TLS) should be allowed. Enabling node-to-node encryption for Elasticsearch domains ensures that intra-cluster communications are encrypted in transit. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1847 | Access Control and Passwords, Identification, Authentication and Passwords, Protecting authentication data in transit (16.1.37.C.01.) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1847 | Access Control and Passwords, Identification, Authentication and Passwords, Protecting authentication data in transit (16.1.37.C.01.) | opensearch-node-to-node-encryption-check | This control checks whether OpenSearch domains have node-to-node encryption enabled. This control fails if node-to-node encryption is disabled on the domain. HTTPS (TLS) can be used to help prevent potential attackers from eavesdropping on or manipulating network traffic using person-in-the-middle or similar attacks. Only encrypted connections over HTTPS (TLS) should be allowed. Enabling node-to-node encryption for OpenSearch domains ensures that intra-cluster communications are encrypted in transit. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1858 | Access Control and Passwords, Identification, Authentication and Passwords, Password selection policy (16.1.40.C.02.) | iam-password-policy | HTTPS (TLS) can be used to help prevent potential attackers from using person-in-the-middle or similar attacks to eavesdrop on or manipulate network traffic. Only encrypted connections over HTTPS (TLS) should be allowed. |
| 1893 | Access Control and Passwords, Identification, Authentication and Passwords, Suspension of access (16.1.46.C.02.) | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule sets maxCredentialUsageAge to 30 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1946 | Access Control and Passwords, Privileged User Access, Use of privileged accounts (16.3.5.C.02.) | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1946 | Access Control and Passwords, Privileged User Access, Use of privileged accounts (16.3.5.C.02.) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 1998 | Access Control and Passwords, Event Logging and Auditing, Maintaining system management logs (16.6.6.C.02.) | cloud-trail-cloud-watch-logs-enabled | You should configure CloudTrail with CloudWatch Logs to monitor your trail logs and be notified when specific activity occurs. This rule checks whether AWS CloudTrail trails are configured to send logs to Amazon CloudWatch logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1998 | Access Control and Passwords, Event Logging and Auditing, Maintaining system management logs (16.6.6.C.02.) | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 1998 | Access Control and Passwords, Event Logging and Auditing, Maintaining system management logs (16.6.6.C.02.) | cw-loggroup-retent ion-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troublesh ooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. The minimum retention is 18 months. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2013 | Access Control and Passwords, Event Logging and Auditing, Additional events to be logged (16.6.10.C.02.) | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2013 | Access Control and Passwords, Event Logging and Auditing, Additional events to be logged (16.6.10.C.02.) | cloudfront-accesslogs-enabled | This control checks whether server access logging is enabled on CloudFront distributions. The control fails if access logging is not enabled for a distribution. CloudFront access logs provide detailed information about every user request that CloudFront receives. Each log contains information such as the date and time the request was received, the IP address of the viewer that made the request, the source of the request, and the port number of the request from the viewer. These logs are useful for applications such as security and access audits and forensics investigation. This rule must be applied in the us-east-1 region. Deploy with template |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | parameter DeployEdgeRules = true |
| 2013 | Access Control and Passwords, Event Logging and Auditing, Additional events to be logged (16.6.10.C.02.) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2013 | Access Control and Passwords, Event Logging and Auditing, Additional events to be logged (16.6.10.C.02.) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2013 | Access Control and Passwords, Event Logging and Auditing, Additional events to be logged (16.6.10.C.02.) | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2013 | Access Control and Passwords, Event Logging and Auditing, Additional events to be logged (16.6.10.C.02.) | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2022 | Access Control and Passwords, Event Logging and Auditing, Event log protection (16.6.12.C.01.) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 2022 | Access Control and Passwords, Event Logging and Auditing, Event log protection (16.6.12.C.01.) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2028 | Access Control and Passwords, Event Logging and Auditing, Event log archives (16.6.13.C.01.) | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. The minimum retention is 18 months. |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. An exemption is available for pre-production environments. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | elasticsearch-encrypted-at-rest | This control checks whether Elasticsearch domains have encryption-at-rest configuration enabled. The check fails if encryption at rest is not enabled. For an added layer of security for sensitive data, you should configure your Elasticsearch Service domain to be encrypted at rest. When you configure encryption of data at rest, AWS KMS stores and manages your encryption keys. To perform the encryption, AWS KMS uses the Advanced Encryption Standard algorithm with 256-bit keys (AES-256). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | encrypted-volumes | Because senstive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | opensearch-encrypted-at-rest | This control checks whether OpenSearch domains have encryption-at-rest configuration enabled. The check fails if encryption at rest is not enabled. For an added layer of security for sensitive data, you should configure your OpenSearch Service domain to be encrypted at rest. When you configure encryption of data at rest, AWS KMS stores and manages your encryption keys. To perform the encryption, AWS KMS uses the Advanced Encryption Standard algorithm with 256-bit keys (AES-256). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2082 | Cryptography, Cryptographic Fundamentals, Reducing storage and physical transfer requirements (17.1.53.C.04.) | s3-default-encryption-kms | To help protect data at rest, ensure that encryption is enabled for your S3 buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. For more information about the encryption process and administration, use the AWS Key Management Service (AWS KMS) customer-managed CMKs. An exemption is available for buckets containing non-sensitive data provided SSE is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2090 | Cryptography, Cryptographic Fundamentals, Information and Systems Protection (17.1.55.C.02.) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2090 | Cryptography, Cryptographic Fundamentals, Information and Systems Protection (17.1.55.C.02.) | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2090 | Cryptography, Cryptographic Fundamentals, Information and Systems Protection (17.1.55.C.02.) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2598 | Cryptography, Transport Layer Security, Using TLS (17.4.16.C.01.) | elb-custom-security-policy-ssl-check | To help protect data in transit, ensure that your Classic ElasticLoadBalancer SSL listeners are using a custom security policy. These policies can provide various high-strength cryptographic algorithms to help ensure encrypted network communications between systems. This rule requires that you set a custom security policy for your SSL listeners. The security policy is: Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2600 | Cryptography, Transport Layer Security, Using TLS (17.4.16.C.02.) | elb-custom-security-policy-ssl-check | To help protect data in transit, ensure that your Classic ElasticLoadBalancer SSL listeners are using a custom security policy. These policies can provide various high-strength cryptographic algorithms to help ensure encrypted network communications between systems. This rule requires that you set a custom security policy for your SSL listeners. The default security policy is: Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2726 | Cryptography, Secure Shell, Automated remote access (17.5.8.C.02.) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3021 | Cryptography, Key Management, Contents of KMPs (17.9.25.C.01.) | cmk-backing-key-rotation-enabled | AWS KMS enables customers to rotate the backing key, which is key material stored in AWS KMS and is tied to the key ID of the CMK. It's the backing key that is used to perform cryptographic operations such as encryption and decryption. Automated key rotation currently retains all previous backing keys so that decryption of encrypted data can take place transparently. Rotating encryption keys helps reduce the potential impact of a compromised key because data encrypted with a new key can't be accessed with a previous key that might have been exposed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3205 | Network security, Network Managemen t, Limiting network access (18.1.13.C.02.) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. The authorized Internet port list is: 443 only |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3449 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .02.) | ec2-managedinstance-patch-compliance-status-check | Enable rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organisation's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3449 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .02.) | ecr-private-image-scanning-enabled | This control checks whether a private ECR repository has image scanning configured. This control fails if a private ECR repositor y doesn't have image scanning configure d. Note that you must also configure scan on push for each repositor y to pass this control. ECR image scanning helps in identifying software vulnerabilities in your container images. ECR uses the Common Vulnerabi lities and Exposures (CVEs) database from the open-sour ce Clair project and provides a list of scan findings. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3449 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .02.) | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule sets allowVersionUpgrade to TRUE. |
| 3451 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .04.) | ec2-managedinstance-patch-compliance-status-check | Enable rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organisation's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3452 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .05.) | ec2-managedinstance-patch-compliance-status-check | Enable rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organisation's policies and procedures. |
| 3452 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .05.) | elastic-beanstalk-managed-updates-enabled | This control checks whether managed platform updates are enabled for the Elastic Beanstalk environment. Enabling managed platform updates ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is an important step in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3452 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .05.) | rds-automatic-minor-version-upgrade-enabled | This control checks whether automatic minor version upgrades are enabled for the RDS database instance. Enabling automatic minor version upgrades ensures that the latest minor version updates to the relational database management system (RDBMS) are installed . These upgrades might include security patches and bug fixes. Keeping up to date with patch installation is an important step in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3453 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .06.) | ec2-managedinstance-patch-compliance-status-check | Enable rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organisation's policies and procedures. |
| 3453 | Product Security, Product Patching and Updating, Patching vulnerabilities in products (12.4.4.C .06.) | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule sets allowVersionUpgrade to TRUE. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. An exemption is available if the load balancer is the origin for a CloudFront distribution with WAF enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | api-gw-associated-with-waf | This control checks whether an API Gateway stage uses a AWS WAF web access control list (ACL). This control fails if a AWS WAF Regional web ACL is not attached to a REST API Gateway stage. AWS WAF is a web application firewall that helps protect web applications and APIs from attacks. It enables you to configure an ACL, which is a set of rules that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure that your API Gateway stage is associated with an AWS WAF web ACL to help protect it from malicious attacks. An exemption is available if the API Gateway is the origin for a CloudFront |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | distribution with WAF enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | cloudfront-associated-with-waf | This control checks whether CloudFront distributions are associated with either AWS WAF or AWS WAFv2 web ACLs. The control fails if the distribution is not associated with a web ACL. AWS WAF is a web application firewall that helps protect web applications and APIs from attacks. It allows you to configure a set of rules, called a web access control list (web ACL), that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your CloudFront distribution is associated with an AWS WAF web ACL to help protect it from malicious attacks. This rule must be applied in the us-east-1 region. Deploy with template |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | parameter DeployEdgeRules = true |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-based controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within anAmazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | elasticsearch-in-vpc-only | This control checks whether Elasticsearch domains are in a VPC. It does not evaluate the VPC subnet routing configuration to determine public access. You should ensure that Elasticsearch domains are not attached to public subnets. Elasticsearch domains deployed within a VPC can communicate with VPC resources over the private AWS network, without the need to traverse the public internet. This configuration increases the security posture by limiting access to the data in transit. VPCs provide a number of network controls to secure access to Elasticsearch domains, including network ACL and security groups |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | opensearch-in-vpc-only | This control checks whether OpenSearch domains are in a VPC. It does not evaluate the VPC subnet routing configuration to determine public access. You should ensure that OpenSearch domains are not attached to public subnets. OpenSearch domains deployed within a VPC can communicate with VPC resources over the private AWS network, without the need to traverse the public internet. This configuration increases the security posture by limiting access to the data in transit. VPCs provide a number of network controls to secure access to OpenSearch domains, including network ACL and security groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule sets ignorePublicAcls to TRUE, blockPublicPolicy to TRUE, blockPublicAcls to TRUE, and restrictPublicBuckets to TRUE. |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3562 | Gateway security, Gateways, Configuration of gateways (19.1.12.C.01.) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3623 | Gateway security, Gateways, Demilitarised zones (19.1.14.C.02.) | elasticsearch-in-vpc-only | This control checks whether Elasticsearch domains are in a VPC. It does not evaluate the VPC subnet routing configuration to determine public access. You should ensure that Elasticsearch domains are not attached to public subnets. Elasticsearch domains deployed within a VPC can communicate with VPC resources over the private AWS network, without the need to traverse the public internet. This configuration increases the security posture by limiting access to the data in transit. VPCs provide a number of network controls to secure access to Elasticsearch domains, including network ACL and security groups |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3623 | Gateway security, Gateways, Demilitarised zones (19.1.14.C.02.) | opensearch-in-vpc-only | This control checks whether OpenSearch domains are in a VPC. It does not evaluate the VPC subnet routing configuration to determine public access. You should ensure that OpenSearch domains are not attached to public subnets. OpenSearch domains deployed within a VPC can communicate with VPC resources over the private AWS network, without the need to traverse the public internet. This configuration increases the security posture by limiting access to the data in transit. VPCs provide a number of network controls to secure access to OpenSearch domains, including network ACL and security groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3623 | Gateway security, Gateways, Demilitarised zones (19.1.14.C.02.) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 3623 | Gateway security, Gateways, Demilitarised zones (19.1.14.C.02.) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3815 | Network security, Intrusion Detection and Prevention, IDS/IPS Maintenance (18.4.9.C.01.) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3857 | Network security, Intrusion Detection and Prevention, Configuring the IDS/IPS (18.4.11.C.01.) | guardduty-eks-protection-audit-enabled | This control checks whether GuardDuty EKS Audit Log Monitoring is enabled. GuardDuty EKS Audit Log Monitoring helps you detect potentially suspicious activities in your Amazon Elastic Kubernetes Service (Amazon EKS) clusters. EKS Audit Log Monitoring uses Kubernetes audit logs to capture chronological activities from users, applications using the Kubernetes API, and the control plane. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3857 | Network security, Intrusion Detection and Prevention, Configuring the IDS/IPS (18.4.11.C.01.) | guardduty-eks-protection-runtime-enabled | This control checks whether GuardDuty EKS Runtime Monitoring with automated agent management is enabled. EKS Protection in Amazon GuardDuty provides threat detection coverage to help you protect Amazon EKS clusters within your AWS environment. EKS Runtime Monitoring uses operating system-level events to help you detect potential threats in EKS nodes and containers within your EKS clusters. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3857 | Network security, Intrusion Detection and Prevention, Configuring the IDS/IPS (18.4.11.C.01.) | guardduty-lambda-protection-enabled | This control checks whether GuardDuty Lambda Protection is enabled. GuardDuty Lambda Protection helps you identify potential security threats when an AWS Lambda function gets invoked. After your enable Lambda Protection, GuardDuty starts monitoring Lambda network activity logs associated with the Lambda functions in your AWS account. When a Lambda function gets invoked and GuardDuty identifies suspicious network traffic that indicates the presence of a potentially malicious piece of code in your Lambda function, GuardDuty generates a finding. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3857 | Network security, Intrusion Detection and Prevention, Configuring the IDS/IPS (18.4.11.C.01.) | guardduty-s3-protection-enabled | This control checks whether GuardDuty S3 Protection is enabled. S3 Protection enables GuardDuty to monitor object-level API operations to identify potential security risks for data within your Amazon S3 buckets. GuardDuty monitors threats against your S3 resources by analyzing AWS CloudTrail management events and CloudTrail S3 data events. |
| 3875 | Network security, Intrusion Detection and Prevention, Event management and correlation (18.4.12.C.01.) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3875 | Network security, Intrusion Detection and Prevention, Event management and correlation (18.4.12. C.01.) | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4333 | Data managemen t, Content Filtering , Content validation (20.3.7.C.02.) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4333 | Data managemen t, Content Filtering , Content validation (20.3.7.C.02.) | api-gw-associated-with-waf | This control checks whether an API Gateway stage uses a AWS WAF web access control list (ACL). This control fails if a AWS WAF Regional web ACL is not attached to a REST API Gateway stage. AWS WAF is a web application firewall that helps protect web applications and APIs from attacks. It enables you to configure an ACL, which is a set of rules that allow, block, or count web requests based on customiza ble web security rules and condition s that you define. Ensure that your API Gateway stage is associated with an AWS WAF web ACL to help protect it from malicious attacks. An exemption is available if the API Gateway is the origin for a CloudFront |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | distribution with WAF enabled. |
| 4441 | Data management, Databases, Database files (20.4.4.C.02.) | elasticsearch-encrypted-at-rest | This control checks whether Elasticsearch domains have encryption-at-rest configuration enabled. The check fails if encryption at rest is not enabled. For an added layer of security for sensitive data, you should configure your Elasticsearch Service domain to be encrypted at rest. When you configure encryption of data at rest, AWS KMS stores and manages your encryption keys. To perform the encryption, AWS KMS uses the Advanced Encryption Standard algorithm with 256-bit keys (AES-256). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4441 | Data management, Databases, Database files (20.4.4.C.02.) | opensearch-encrypted-at-rest | This control checks whether OpenSearch domains have encryption-at-rest configuration enabled. The check fails if encryption at rest is not enabled. For an added layer of security for sensitive data, you should configure your OpenSearch Service domain to be encrypted at rest. When you configure encryption of data at rest, AWS KMS stores and manages your encryption keys. To perform the encryption, AWS KMS uses the Advanced Encryption Standard algorithm with 256-bit keys (AES-256). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4441 | Data management, Databases, Database files (20.4.4.C.02.) | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |
| 4441 | Data management, Databases, Database files (20.4.4.C.02.) | rds-snapshot-encry pted | Ensure that encryptio n is enabled for your Amazon Relationa l Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4441 | Data management, Databases, Database files (20.4.4.C.02.) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 4441 | Data management, Databases, Database files (20.4.4.C.02.) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4441 | Data management, Databases, Database files (20.4.4.C.02.) | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule sets clusterDbEncrypted to TRUE, and loggingEnabled to TRUE. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4445 | Data management, Databases, Accountability (20.4.5.C.02.) | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4445 | Data management, Databases, Accountability (20.4.5.C.02.) | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule sets clusterDbEncrypted to TRUE, and loggingEnabled to TRUE. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4829 | Enterprise systems security, Cloud Computing, System Availability (22.1.23.C.01.) | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4829 | Enterprise systems security, Cloud Computing, System Availability (22.1.23.C.01.) | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4829 | Enterprise systems security, Cloud Computing, System Availability (22.1.23.C.01.) | rds-cluster-multi-az-enabled | Amazon Aurora stores copies of the data in a DB cluster across multiple Availability Zones in a single AWS Region. Aurora stores these copies regardles s of whether the instances in the DB cluster span multiple Availability Zones. When data is written to the primary DB instance, Aurora synchronously replicates the data across Availability Zones to six storage nodes associated with your cluster volume. Doing so provides data redundanc y, eliminates I/O freezes, and minimizes latency spikes during system backups. Running a DB instance with high availability can enhance availabil ity during planned system maintenan ce, and help protect |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | your databases against failure and Availability Zone disruption. This rule checks if Multi-AZ replication is enabled on Amazon Aurora clusters managed by Amazon RDS. An exemption is available for pre-production environments. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4829 | Enterprise systems security, Cloud Computing, System Availability (22.1.23.C.01.) | rds-multi-az-support | Multi-AZ support in Amazon Relational Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availability Zone. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operations as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | An exemption is available for pre-production environments. |
| 4838 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.03.) | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| 4838 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.03.) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4838 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.03.) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule sets ignorePublicAcls to TRUE, blockPublicPolicy to TRUE, blockPublicAcls to TRUE, and restrictPublicBuckets to TRUE. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4838 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.03.) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 4838 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.03.) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | elasticsearch-encrypted-at-rest | This control checks whether Elasticsearch domains have encryption-at-rest configuration enabled. The check fails if encryption at rest is not enabled. For an added layer of security for sensitive data, you should configure your Elasticsearch Service domain to be encrypted at rest. When you configure encryption of data at rest, AWS KMS stores and manages your encryption keys. To perform the encryption, AWS KMS uses the Advanced Encryption Standard algorithm with 256-bit keys (AES-256). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | elasticsearch-node-to-node-encryption-check | This control checks whether Elasticsearch domains have node-to-node encryption enabled. This control fails if node-to-node encryption is disabled on the domain. HTTPS (TLS) can be used to help prevent potential attackers from eavesdropping on or manipulat ing network traffic using person-in -the-middle or similar attacks. Only encrypted connectio ns over HTTPS (TLS) should be allowed. Enabling node-to-n ode encryption for Elasticsearch domains ensures that intra-cluster communica tions are encrypted in transit. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | encrypted-volumes | Because senstive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | opensearch-encrypted-at-rest | This control checks whether OpenSearch domains have encryption-at-rest configuration enabled. The check fails if encryption at rest is not enabled. For an added layer of security for sensitive data, you should configure your OpenSearch Service domain to be encrypted at rest. When you configure encryption of data at rest, AWS KMS stores and manages your encryption keys. To perform the encryption, AWS KMS uses the Advanced Encryption Standard algorithm with 256-bit keys (AES-256). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | opensearch-node-to-node-encryption-check | This control checks whether OpenSearch domains have node-to-node encryption enabled. This control fails if node-to-node encryption is disabled on the domain. HTTPS (TLS) can be used to help prevent potential attackers from eavesdropping on or manipulating network traffic using person-in-the-middle or similar attacks. Only encrypted connections over HTTPS (TLS) should be allowed. Enabling node-to-node encryption for OpenSearch domains ensures that intra-cluster communications are encrypted in transit. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule sets clusterDbEncrypted to TRUE, and loggingEnabled to TRUE. |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4839 | Enterprise systems security, Cloud Computing, Unauthorised Access (22.1.24.C.04.) | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. An exemption is available when messages published to the topic do not contain sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. An exemption is available when a compensating recovery solution has been configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. An exemption is available when a compensating recovery solution has been configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. An exemption is available when a compensating recovery solution has been configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | rds-cluster-deletion-protection-enabled | Ensure Amazon RDS instances have deletion protection enabled. Use deletion protection to prevent your RDS instances from being accidenta lly or malicious ly deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup complianc e requirements. An exemption is available when a compensating recovery solution has been configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protection enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB per node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4849 | Enterprise systems security, Cloud Computing, Backup, Recovery Archiving and Data Remanence (22.1.26.C.01.) | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. An exemption is available when only a single variant of an object will be created, or when a compensat ing recovery solution has been configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6843 | Access Control and Passwords, Privileged Access Management, The Principle of Least Privilege (16.4.31. C.02.) | mfa-enabled-for-iam-console-access | MFA adds extra security by requiring users to provide unique authentication from an AWS-supported MFA mechanism - in addition to their regular sign-in credentials - when they access AWS websites or services. Supported mechanisms include U2F security keys, virtual or hardware MFA devices, and SMS-based codes. This rule checks whether AWS Multi-Factor Authentication (MFA) is enabled for all AWS Identity and Access Management (IAM) users that use a console password. The rule is compliant if MFA is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6843 | Access Control and Passwords, Privileged Access Management, The Principle of Least Privilege (16.4.31. C.02.) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6852 | Access Control and Passwords, Privileged Access Management, Suspension and Revocation of Privileged Access Credentials (16.4.33.C.01.) | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule sets maxCredentialUsageAge to 30 days. |
| 6860 | Access Control and Passwords, Privileged Access Management, Monitoring and Review (16.4.35.C.02.) | cloud-trail-cloud-watch-logs-enabled | You should configure CloudTrail with CloudWatch Logs to monitor your trail logs and be notified when specific activity occurs. This rule checks whether AWS CloudTrail trails are configured to send logs to Amazon CloudWatch logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6860 | Access Control and Passwords, Privileged Access Management, Monitoring and Review (16.4.35.C.02.) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 6861 | Access Control and Passwords, Privileged Access Management, Monitoring and Review (16.4.35.C.03.) | cloudtrail-security-trail-enabled | This rule helps ensure the use of AWS recommended security best practices for AWS CloudTrail, by checking for the enablement of multiple settings. These include the use of log encryption, log validation, and enabling AWS CloudTrail in multiple regions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6953 | Access Control and Passwords, Multi-Factor Authentication, System Architecture and Security Controls (16.7.34.C.02.) | mfa-enabled-for-iam-console-access | MFA adds extra security by requiring users to provide unique authentication from an AWS-supported MFA mechanism - in addition to their regular sign-in credentials - when they access AWS websites or services. Supported mechanisms include U2F security keys, virtual or hardware MFA devices, and SMS-based codes. This rule checks whether AWS Multi-Factor Authentication (MFA) is enabled for all AWS Identity and Access Management (IAM) users that use a console password. The rule is compliant if MFA is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6953 | Access Control and Passwords, Multi-Factor Authentication, System Architecture and Security Controls (16.7.34.C.02.) | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 7436 | Public Cloud Security, Identity Management and Access Control, Username and passwords (23.3.19.C.01.) | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7436 | Public Cloud Security, Identity Managemen t and Access Control, Username and passwords (23.3.19. C.01.) | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protectio n on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7436 | Public Cloud Security, Identity Managemen t and Access Control, Username and passwords (23.3.19. C.01.) | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7436 | Public Cloud Security, Identity Managemen t and Access Control, Username and passwords (23.3.19. C.01.) | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 7437 | Public Cloud Security, Identity Managemen t and Access Control, Username and passwords (23.3.19. C.01.) | iam-user-mfa-enabl ed | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-fac tor authentication (MFA) is enabled for all IAM users. MFA adds an extra layer of protectio n on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for IAM users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7437 | Public Cloud Security, Identity Managemen t and Access Control, Username and passwords (23.3.19. C.01.) | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protectio n on top of a user name and password. By requiring MFA for IAM users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7437 | Public Cloud Security, Identity Managemen t and Access Control, Username and passwords (23.3.19. C.01.) | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7437 | Public Cloud Security, Identity Managemen t and Access Control, Username and passwords (23.3.19. C.01.) | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10. C.01.) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | api-gw-associated-with-waf | This control checks whether an API Gateway stage uses a AWS WAF web access control list (ACL). This control fails if a AWS WAF Regional web ACL is not attached to a REST API Gateway stage. AWS WAF is a web application firewall that helps protect web applications and APIs from attacks. It enables you to configure an ACL, which is a set of rules that allow, block, or count web requests based on customiza ble web security rules and condition s that you define. Ensure that your API Gateway stage is associated with an AWS WAF web ACL to help protect it from malicious attacks. An exemption is available if the API Gateway is the origin for a CloudFront |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | distribution with WAF enabled. |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10. C.01.) | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within anAmazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | elasticsearch-in-vpc-only | This control checks whether Elasticsearch domains are in a VPC. It does not evaluate the VPC subnet routing configuration to determine public access. You should ensure that Elasticsearch domains are not attached to public subnets. Elasticsearch domains deployed within a VPC can communicate with VPC resources over the private AWS network, without the need to traverse the public internet. This configuration increases the security posture by limiting access to the data in transit. VPCs provide a number of network controls to secure access to Elasticsearch domains, including network ACL and security groups |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | opensearch-in-vpc-only | This control checks whether OpenSearch domains are in a VPC. It does not evaluate the VPC subnet routing configuration to determine public access. You should ensure that OpenSearch domains are not attached to public subnets. OpenSearch domains deployed within a VPC can communicate with VPC resources over the private AWS network, without the need to traverse the public internet. This configuration increases the security posture by limiting access to the data in transit. VPCs provide a number of network controls to secure access to OpenSearch domains, including network ACL and security groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule sets ignorePublicAcls to TRUE, blockPublicPolicy to TRUE, blockPublicAcls to TRUE, and restrictPublicBuckets to TRUE. |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7466 | Public Cloud Security, Data Protection in Public Cloud, Data accessibility (23.4.10.C.01.) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requirements (23.5.11.C.01.) | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requirements (23.5.11.C.01.) | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requirements (23.5.11.C.01.) | cloudfront-accesslogs-enabled | This control checks whether server access logging is enabled on CloudFront distributions. The control fails if access logging is not enabled for a distribution. CloudFront access logs provide detailed information about every user request that CloudFront receives. Each log contains information such as the date and time the request was received, the IP address of the viewer that made the request, the source of the request, and the port number of the request from the viewer. These logs are useful for applications such as security and access audits and forensics investigation. This rule must be applied in the us-east-1 region. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requirements (23.5.11.C.01.) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requirements (23.5.11.C.01.) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requirements (23.5.11.C.01.) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requireme nts (23.5.11.C.01.) | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7496 | Public Cloud Security, Logging and Alerting in Public Cloud, Logging requirements (23.5.11.C.01.) | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

### Template

The template is available on GitHub: Operational Best Practices for NZISM.

## Operational Best Practices for PCI DSS 3.2.1

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more PCI DSS controls. A PCI DSS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | alb-desync-mode-check | To assist in protecting applications for HTTP Desync vulnerabilities, ensure HTTP Desync mitigation mode is enabled on your application load balancers. HTTP Desync issues can lead to request smuggling and make your applications vulnerable to request queue or cache poisoning. Desync mitigation modes are monitor, defensive, and strictest. Defensive is the default mode. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | to help protect that data. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | netfw-stateless-rule-group-not-empty | An AWS Network Firewall rule group contains rules that define how your firewall processes traffic in your VPC. An empty stateless rule group when present in a firewall policy does not process traffic. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3 | Prohibit direct public access between the Internet and any system component in the cardholder data environment. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | netfw-policy-rule-group-associated | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows, and you define default traffic handling. |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | netfw-stateless-rule-group-not-empty | An AWS Network Firewall rule group contains rules that define how your firewall processes traffic in your VPC. An empty stateless rule group when present in a firewall policy does not process traffic. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholde r data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholde r data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.6 | Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.). | rds-cluster-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Relational Database Service (Amazon RDS) database cluster(s). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.). | rds-instance-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Relational Database Service (Amazon RDS) database instance(s). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.). | redshift-default-admin-check | As default usernames are public knowledge, changing default usernames can assist in reducing the attack surface for your Amazon Redshift cluster(s). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessa ry default accounts before installin g a system on the network. This applies to ALL default passwords , including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Managemen t Protocol (SNMP) community strings, etc.). | redshift-default-db-name-check | Default names are public knowledge and should be changed upon configuration. Changing the default database name of your Amazon Redshift cluster can assist in reducing the attack surface for your Redshift cluster. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.1 | Always change vendor-supplied defaults and remove or disable unnecessa ry default accounts before installin g a system on the network. This applies to ALL default passwords , including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Managemen t Protocol (SNMP) community strings, etc.). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | ec2-instance-multiple-eni-check | This rule checks if your Amazon Elastic Compute Cloud (Amazon EC2) instances have multiple ENIs. Having multiple ENIs can cause dual-homed instances, meaning instances that have multiple subnets. This can add network security complexity and introduce unintended network paths and access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: ,Ä¢ Center for Internet Security (CIS) ,Ä¢ International Organization for Standardization (ISO) ,Ä¢ SysAdmin Audit Network Security (SANS) Institute ,Ä¢ National Institute of Standards Technology (NIST). | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of a user name and password. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2 | Develop configura tion standards for all system component s. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technolog y (NIST). | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: ,Ä¢ Center for Internet Security (CIS) ,Ä¢ International Organization for Standardization (ISO) ,Ä¢ SysAdmin Audit Network Security (SANS) Institute ,Ä¢ National Institute of Standards Technology (NIST). | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2 | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST). | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints.<br>To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.2 | Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.3 | Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. | alb-desync-mode-check | To assist in protecting applications for HTTP Desync vulnerabilities, ensure HTTP Desync mitigation mode is enabled on your application load balancers. HTTP Desync issues can lead to request smuggling and make your applications vulnerable to request queue or cache poisoning. Desync mitigation modes are monitor, defensive, and strictest. Defensive is the default mode. |
| 2.3 | Encrypt all non-console administrative access using strong cryptography. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.3 | Encrypt all non-conso le administrative access using strong cryptography. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |
| 2.3 | Encrypt all non-conso le administrative access using strong cryptography. | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.3 | Encrypt all non-conso le administrative access using strong cryptography. | opensearch-https-r equired | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.3 | Encrypt all non-conso le administrative access using strong cryptography. | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryptio n to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 2.4 | Maintain an inventory of system component s that are in scope for PCI DSS. | ec2-security-group-attached-to-eni-periodic | This rule ensures the security groups are attached to an Amazon Elastic Compute Cloud (Amazon EC2) instance or to an ENI. This rule helps monitoring unused security groups in the inventory and the management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.4 | Maintain an inventory of system component s that are in scope for PCI DSS. | eip-attached | This rule ensures Elastic IPs allocated to a Amazon Virtual Private Cloud (Amazon VPC) are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances or in-use Elastic Network Interfaces. This rule helps monitor unused EIPs in your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.4 | Maintain an inventory of system components that are in scope for PCI DSS. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 2.4 | Maintain an inventory of system components that are in scope for PCI DSS. | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1 | Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | s3-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1 | Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1 | Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1 | Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4 | Render PAN unreadable anywhere it is stored (includin g on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptogra phy, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptogra phy with associate d key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individua l to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (includin g on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptogra phy, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptogra phy with associate d key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individua l to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (includin g on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptogra phy, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptogra phy with associate d key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individua l to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4 | Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.4 | Render PAN unreadable anywhere it is stored (includin g on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptogra phy, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptogra phy with associate d key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individua l to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | sagemaker-notebook -instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.4 | Render PAN unreadable anywhere it is stored (includin g on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptogra phy, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptogra phy with associate d key-management processes and procedures. Note: It is a relatively trivial effort for a malicious individua l to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.2 | Restrict access to cryptographic keys to the fewest number of custodians necessary. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.2 | Restrict access to cryptographic keys to the fewest number of custodians necessary. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.3 | Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data- encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry- accepted method Note: It is not required that public keys be stored in one of these forms. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.3 | Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data- encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry- accepted method Note: It is not required that public keys be stored in one of these forms. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.3 | Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data- encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry- accepted method Note: It is not required that public keys be stored in one of these forms. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.4 | Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.5 | Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.7 | Prevention of unauthorized substitution of cryptographic keys. | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | elb-tls-https-list eners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | elbv2-acm-certific ate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | opensearch-https-r equired | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | opensearch-node-to -node-encryption-c heck | Ensure node-to-node encryptio n for Amazon OpenSearch Service is enabled. Node-to-node encryptio n enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.1 | Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.1 | Use strong cryptogra phy and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropria te for the encryptio n methodology in use. Examples of open, public networks include but are not limited to: • The Internet • Wireless technolog ies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access | s3-bucket-ssl-requ ests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | (CDMA) • General Packet Radio Service (GPRS) • Satellite communications | | |
| 6.2 | Ensure that all system component s and software are protected from known vulnerabilities by installing applicabl e vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environme nt ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.2 | Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.2 | Ensure that all system component s and software are protected from known vulnerabilities by installing applicabl e vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | ec2-managedinstanc e-patch-compliance-status-check | Enable this rule to help with identific ation and documenta tion of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch complianc e in AWS Systems Manager as required by your organizat ion's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.2 | Ensure that all system component s and software are protected from known vulnerabilities by installing applicabl e vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | ecs-fargate-latest-platform-version | Security updates and patches are deployed automatic ally for your AWS Fargate tasks. If a security issue is found that affects an AWS Fargate platform version, AWS patches the platform version. To assist in patch management of your Amazon Elastic Container Service (ECS) tasks running AWS Fargate, update your services standalone tasks to use the most recent platform version. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.2 | Ensure that all system component s and software are protected from known vulnerabilities by installing applicabl e vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | rds-automatic-mino r-version-upgrade- enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed , which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.2 | Ensure that all system component s and software are protected from known vulnerabilities by installing applicabl e vendor- supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1. | redshift-cluster-m aintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organizat ion. Specifically, that they have preferred maintenan ce windows and automated snapshot retention periods for the database. This rule requires you to set the allowVers ionUpgrade. The default is true. It also lets you optionall y set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionP eriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.3.2 | Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release. (Continued on next page) | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications from manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applicati | alb-desync-mode-check | To assist in protecting applications for HTTP Desync vulnerabilities, ensure HTTP Desync mitigation mode is enabled on your application load balancers. HTTP Desync issues can lead to request smuggling and make your applications vulnerable to request queue or cache poisoning. Desync mitigation modes are monitor, defensive, and strictest. Defensive is the default mode. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ons, to continually check all traffic. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications from manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applicati | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ons, to continually check all traffic. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications from manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applicati | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ons, to continually check all traffic. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications from manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applicati | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no conditions could result in unintended behavior. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ons, to continually check all traffic. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications from manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applicati | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | ons, to continually check all traffic. | | |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.6 | For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications from manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applicati | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collection of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | ons, to continually check all traffic. | | |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | ecs-containers-non privileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitio ns should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | ecs-containers-rea donly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance' s filesystem cannot be modified unless it has explicit read-writ e permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.1 | Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-user-group-mem bership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.1.2 | Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Managemen t (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportuni ty for an identity to receive or retain excessive privileges. |
| 7.2.1 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following : Coverage of all system components | ecs-containers-non privileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitio ns should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following : Coverage of all system components | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following : Coverage of all system components | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following : Coverage of all system components | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following : Coverage of all system components | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Coverage of all system components | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | ecs-containers-nonprivileged | To assist with implementing the principle of least privilege, Amazon Elastic Container Service (Amazon ECS) task definitions should not have elevated privilege enabled. When this parameter is true, the container is given elevated privileges on the host container instance (similar to the root user). |
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | ecs-containers-readonly-access | Enabling read only access to Amazon Elastic Container Service (ECS) containers can assist in adhering to the principal of least privilege. This option can reduces attack vectors as the container instance's filesystem cannot be modified unless it has explicit read-write permissions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | information about each principal. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignmen t of privileges to individuals based on job classification and function. | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, restricti ng policies from containing blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignmen t of privileges to individuals based on job classification and function. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignmen t of privileges to individuals based on job classification and function. | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Managemen t Service keys. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegatin g permissions management. This rule allows you to set the blockedAc tionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom) . The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignmen t of privileges to individuals based on job classification and function. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.2 | Establish an access control system(s) for systems component s that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignmen t of privileges to individuals based on job classification and function. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: Assignment of privileges to individuals based on job classification and function. | opensearch-access-control-enabled | Ensure fine-grained access control is enabled on your Amazon OpenSearch Service domains. Fine-grained access control provides enhanced authorization mechanisms to achieve least-privileged access to Amazon OpenSearch Service domains. It allows for role-based access control to the domain, as well as index, document, and field-level security, support for OpenSearch Service dashboards multi-tenancy, and HTTP basic authentication for OpenSearch Service and Kibana. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.3 | Default “deny-all” setting. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1.1 | Assign all users a unique ID before allowing them to access system components or cardholder data. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1.4 | Remove/disable inactive user accounts within 90 days. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | codebuild-project-environment-privileged-check | To assist with implementing the principle of least privilege, ensure your Amazon CodeBuild project environment does not have privileged mode enabled. This setting should be disabled to prevent unintended access to Docker APIs as well as the container's underlying hardware. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | ecs-no-environment-secrets | As a security best practice, pass sensitive informati on to container s as environme nt variables. You can securely inject data into your Amazon Elastic Container Service (ECS) container s by referencing values stored in AWS Systems Manager Parameter Store or AWS Secrets Manager in the container definition of an Amazon ECS task definition. Then, you can expose your sensitive informati on as environment variables or in the log configuration of a container. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Applicati on Load Balancer automatically redirects unencrypt ed HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configure d with SSL certifica tes to allow backend systems to authentic ate that requests originate from API Gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon Elastic File System (EFS). |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryptio n is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryption at rest to help protect that data. |
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2.1 | Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.3 | Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (PCI DSS default: false), RequireLowercaseCharacters (PCI DSS default: true), RequireSymbols (PCI DSS default: false), RequireNumbers (PCI DSS default: true), MinimumPasswordLength (PCI DSS default: 7), PasswordReusePrevention (PCI DSS default: 4), and MaxPasswordAge (PCI DSS default: 90) for |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | your IAM Password Policy. The actual values should reflect your organization's policies. |
| 8.2.4 | Change user passwords/passphrases at least after every 90 days. | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.4 | Change user passwords/passphrases at least after every 90 days. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundational Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCharacters (PCI DSS default: false), RequireLowercaseCharacters (PCI DSS default: true), RequireSymbols (PCI DSS default: false), RequireNumbers (PCI DSS default: true), MinimumPasswordLength (PCI DSS default: 7), PasswordReusePrevention (PCI DSS default: 4), and MaxPasswordAge (PCI DSS default: 90) for |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | your IAM Password Policy. The actual values should reflect your organization's policies. |
| 8.2.4 | Change user passwords/passphrases at least after every 90 days. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.5 | Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (PCI DSS default: false), RequireLowercaseCh aracters (PCI DSS default: true), RequireSymbols (PCI DSS default: false), RequireNumbers (PCI DSS default: true), MinimumPa sswordLength (PCI DSS default: 7), PasswordReusePreve ntion (PCI DSS default: 4), and MaxPasswordAge (PCI DSS default: 90) for |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | your IAM Password Policy. The actual values should reflect your organization's policies. |
| 8.3.1 | Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.3.1 | Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protectio n on top of a user name and password. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.1 | Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.3.1 | Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 8.3.2 | Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of a user name and password. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Incorporate multi-factor authentic ation for all remote network access (both user and administr ator, and including third-party access for support or maintenan ce) originating from outside the entity's network. | mfa-enabled-for-ia m-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protectio n on top of a user name and password. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Incorporate multi-factor authentic ation for all remote network access (both user and administr ator, and including third-party access for support or maintenan ce) originating from outside the entity's network. | root-account-hardw are-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privilege d user in an AWS account. The MFA adds an extra layer of protection for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Incorporate multi-factor authentic ation for all remote network access (both user and administr ator, and including third-party access for support or maintenan ce) originating from outside the entity's network. | root-account-mfa-e nabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for a user name and password. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 10.1 | Implement audit trails to link all access to system component s to each individual user. | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system component s to each individual user. | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system component s to each individual user. | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 10.1 | Implement audit trails to link all access to system component s to each individual user. | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.1 | Implement audit trails to link all access to system components to each individual user. | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.6 | Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.6 | Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.2.6 | Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system- level objects | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system- level objects | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system- level objects | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system- level objects | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system- level objects | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system- level objects | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system- level objects | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identific ation | api-gw-execution-l ogging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identific ation | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identific ation | wafv2-logging-enab led | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identific ation | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identific ation | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identific ation | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Record at least the following audit trail entries for all system components for each event: User identification | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| 10.5 | Secure audit trails so they cannot be altered. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.5 | Secure audit trails so they cannot be altered. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 10.5 | Secure audit trails so they cannot be altered. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| 10.5.2 | Protect audit trail files from unauthorized modifications. | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.5.2 | Protect audit trail files from unauthorized modifications. | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 10.5.2 | Protect audit trail files from unauthorized modifications. | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | s3-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.5.5 | Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.5.5 | Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |
| 10.7 | Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorabl e from backup). | s3-lifecycle-policy-check | Ensure Amazon S3 lifecycle policies are configured to help define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7 | Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.2.3 | Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. | ecr-private-image-scanning-enabled | Amazon Elastic Container Repository (ECR) image scanning assists in identifying software vulnerabilities in your container images. Enabling image scanning on ECR repositories adds a layer of verification for the integrity and safety of the images being stored. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.4 | Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date. | netfw-policy-rule-group-associated | An AWS Network Firewall policy defines how your firewall monitors and handles traffic in an Amazon VPC. You configure stateless and stateful rule groups to filter packets and traffic flows, and you define default traffic handling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.5 | Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.5 | Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

### Template

The template is available on GitHub: Operational Best Practices for PCI DSS 3.2.1.

## Operational Best Practices for PCI DSS 4.0 (Excluding global resource types)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates,

are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Payment Card Industry Data Security Standard (PCI DSS) 4.0 (Excluding global resource types) and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more PCI DSS controls. A PCI DSS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.5 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | transfer-family-server-no-ftp | Ensure that a server created with AWS Transfer Family does not use FTP for endpoint connection. The rule is NON_COMPLIANT if the server protocol for endpoint connection is FTP-enabled. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifie r (INCOMING _SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGroupRuleRanges. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifier (INCOMING_SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifier (INCOMING_SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 1.4.1 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.4.1 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.4.1 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifie r (INCOMING _SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGroupRuleRanges. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 1.4.3 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.3 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.4.3 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-full-packets | Ensure that an AWS Network Firewall policy is configured with a user defined default stateless action for full packets. This rule is NON_COMPLIANT if default stateless action for full packets does not match with user defined default stateless action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.4.4 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |
| 1.4.4 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.4.4 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.5 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | ecs-task-definition-pid-mode-check | Ensure that ECSTaskDefinitions are configured to share a host's process namespace with its Amazon Elastic Container Service (Amazon ECS) containers. The rule is NON_COMPLIANT if the pidMode parameter is set to 'host'. |
| 1.4.5 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | ec2-launch-template-public-ip-disabled | Ensure that Amazon EC2 Launch Templates are not set to assign public IP addresses to Network Interfaces. The rule is NON_COMPLIANT if the default version of an EC2 Launch Template has at least 1 Network Interface with 'AssociatePublicIpAddress' set to 'true'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifier (INCOMING_SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | emr-block-public-a ccess | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurit yGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGrou pRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGroupRuleRanges. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | aurora-resources-protected-by-backup-plan | Ensure that Amazon Aurora DB clusters are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon Relational Database Service (Amazon RDS) Database Cluster is not protected by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | db-instance-backup-enabled | Ensure that RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | dynamodb-in-backup-plan | Ensure that Amazon DynamoDB tables are present in AWS Backup Plans. The rule is NON_COMPLIANT if Amazon DynamoDB tables are not present in any AWS Backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | dynamodb-resources-protected-by-backup-plan | Ensure that Amazon DynamoDB tables are protected by a backup plan. The rule is NON_COMPLIANT if the DynamoDB Table is not covered by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ebs-in-backup-plan | Ensure that Amazon Elastic Block Store (Amazon EBS) volumes are added in backup plans of AWS Backup. The rule is NON_COMPLIANT if Amazon EBS volumes are not included in backup plans. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ebs-resources-protected-by-backup-plan | Ensure that Amazon Elastic Block Store (Amazon EBS) volumes are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon EBS volume is not covered by a backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ec2-resources-protected-by-backup-plan | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) instances are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon EC2 instance is not covered by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | efs-resources-protected-by-backup-plan | Ensure that Amazon Elastic File System (Amazon EFS) file systems are protected by a backup plan. The rule is NON_COMPLIANT if the EFS File System is not covered by a backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | elasticache-redis-cluster-automatic-backup-check | Check if the Amazon ElastiCache Redis clusters have automatic backup turned on. The rule is NON_COMPLIANT if the SnapshotRetentionLimit for Redis cluster is less than the SnapshotRetentionPeriod parameter. For example: If the parameter is 15 then the rule is non-compliant if the snapshotRetentionPeriod is between 0-15. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | fsx-resources-protected-by-backup-plan | Ensure that Amazon FSx File Systems are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon FSx File System is not covered by a backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | neptune-cluster-backup-retention-check | Ensure that an Amazon Neptune DB cluster retention period is set to specific number of days. The rule is NON_COMPLIANT if the retention period is less than the value specified by the parameter. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | rds-in-backup-plan | Ensure that Amazon Relational Database Service (Amazon RDS) databases are present in AWS Backup plans. The rule is NON_COMPLIANT if Amazon RDS databases are not included in any AWS Backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | redshift-backup-enabled | Ensure that Amazon Redshift automated snapshots are enabled for clusters. The rule is NON_COMPLIANT if the value for automated SnapshotRetentionPeriod is greater than MaxRetentionPeriod or less than MinRetentionPeriod or the value is 0. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-resources-protected-by-backup-plan | Ensure that Amazon Simple Storage Service (Amazon S3) buckets are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon S3 bucket is not covered by a backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | db-instance-backup-enabled | Ensure that RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-bucket-default-lock-enabled | Ensure that the S3 bucket has lock enabled, by default. The rule is NON_COMPLIANT if the lock is not enabled. |
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-bucket-versioning-enabled | Ensure that versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.4.3 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repositor y. |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPL IANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 12.4.2.1 | PCI DSS compliance is managed. (PCI-DSS-v4.0) | service-catalog-shared-within-organization | Ensure that AWS Service Catalog shares portfolios to an organization (a collection of AWS accounts treated as a single unit) when integration is enabled with AWS Organizations. The rule is NON_COMPLIANT if the `Type` value of a share is `ACCOUNT`. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.5 | System components are configured and managed securely. (PCI-DSS-v4.0) | transfer-family-server-no-ftp | Ensure that a server created with AWS Transfer Family does not use FTP for endpoint connection. The rule is NON_COMPLIANT if the server protocol for endpoint connection is FTP-enabled. |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | dms-redis-tls-enabled | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL encryption is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | athena-workgroup-encrypted-at-rest | Ensure that an Amazon Athena workgroup is encrypted at rest. The rule is NON_COMPLIANT if encryption of data at rest is not enabled for an Athena workgroup. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | neptune-cluster-snapshot-encrypted | Ensure that an Amazon Neptune DB cluster has snapshots encrypted. The rule is NON_COMPLIANT if a Neptune cluster does not have snapshots encrypted. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | redshift-cluster-kms-enabled | Ensure that Amazon Redshift clusters are using a specified AWS Key Management Service (AWS KMS) key for encryptio n. The rule is COMPLIANT if encryption is enabled and the cluster is encrypted with the key provided in the kmsKeyArn parameter. The rule is NON_COMPL IANT if the cluster is not encrypted or encrypted with another key. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | codebuild-project-s3-logs-encrypted | Ensure that an AWS CodeBuild project configured with Amazon S3 Logs has encryption enabled for its logs. The rule is NON_COMPLIANT if 'encryptionDisable d' is set to 'true' in a S3LogsConfig of a CodeBuild project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | eks-secrets-encrypted | Ensure that Amazon Elastic Kubernetes Service clusters are configured to have Kubernetes secrets encrypted using AWS Key Management Service (KMS) keys. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | api-gw-cache-enabled-and-encrypted | Ensure that all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in an Amazon API Gateway stage is not configured to cache or the cache is not encrypted. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | dynamodb-table-encrypted-kms | Ensure that Amazon DynamoDB table is encrypted with AWS Key Management Service (KMS). The rule is NON_COMPLIANT if Amazon DynamoDB table is not encrypted with AWS KMS. The rule is also NON_COMPLIANT if the encrypted AWS KMS key is not present in kmsKeyArns input parameter. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | codebuild-project-envvar-awscred-check | Ensure that the project DOES NOT contain environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | eks-cluster-secrets-encrypted | Ensure that Amazon EKS clusters are not configured to have Kubernetes secrets encrypted using AWS KMS. The rule is NON_COMPLIANT if an EKS cluster does not have an encryptionConfig resource or if encryptionConfig does not name secrets as a resource. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | kinesis-stream-encrypted | Ensure that Amazon Kinesis streams are encrypted at rest with server-side encryption. The rule is NON_COMPLIANT for a Kinesis stream if 'StreamEncryption' is not present. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | neptune-cluster-encrypted | Ensure that storage encryption is enabled for your Amazon Neptune DB clusters. The rule is NON_COMPLIANT if storage encryption is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.5.1.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.6.1 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1.2 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.6.1.2 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1.3 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.6.1.3 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1.4 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.6.1.4 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.1 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-certificate-rsa-check | Ensure that RSA certificates managed by AWS Certificate Manager (ACM) have a key length of at least '2048' bits.The rule is NON_COMPL IANT if the minimum key length is less than 2048 bits. |
| 3.7.1 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.1 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.7.2 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.2 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.7.4 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.4 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.7.6 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.6 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.7.7 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.7 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-redis-tls-enab led | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPL IANT if TLS/SSL encryption is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryptio n in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communica tion is enabled for in-cluster broker node connections. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-redis-tls-enabled | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL encryption is not enabled. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 6.3.3 | Security vulnerabilities are identified and addressed. (PCI-DSS-v4.0) | lambda-function-settings-check | Ensure that the AWS Lambda function settings for runtime, role, timeout, and memory size match the expected values. The rule ignores functions with the 'Image' package type and functions with runtime set to 'OS-only Runtime'. The rule is NON_COMPLIANT if the Lambda function settings do not match the expected values. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3.3 | Security vulnerabilities are identified and addressed. (PCI-DSS-v4.0) | eks-cluster-oldest-supported-version | Ensure that an Amazon Elastic Kubernetes Service (EKS) cluster is not running the oldest supported version. The rule is NON_COMPLIANT if an EKS cluster is running oldest supported version (equal to the parameter 'oldestVersionSupported'). |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-webacl-not-empty | Ensure that a WAFv2 Web ACL contains any WAF rules or WAF rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rules or WAF rule groups. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-rulegroup-not-empty | Ensure that WAFv2 Rule Groups contain rules. The rule is NON_COMPLIANT if there are no rules in a WAFv2 Rule Group. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-webacl-not-empty | Ensure that a WAFv2 Web ACL contains any WAF rules or WAF rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rules or WAF rule groups. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-rulegroup-not-empty | Ensure that WAFv2 Rule Groups contain rules. The rule is NON_COMPLIANT if there are no rules in a WAFv2 Rule Group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.5.5 | Changes to all system components are managed securely. (PCI-DSS-v4.0) | codedeploy-lambda-allatonce-traffic-shift-disabled | Ensure that the deployment group for Lambda Compute Platform is not using the default deployment configuration. The rule is NON_COMPLIANT if the deployment group is using the deployment configuration 'CodeDeployDefault.LambdaAllAtOnce'. |
| 6.5.6 | Changes to all system components are managed securely. (PCI-DSS-v4.0) | codedeploy-lambda-allatonce-traffic-shift-disabled | Ensure that the deployment group for Lambda Compute Platform is not using the default deployment configuration. The rule is NON_COMPLIANT if the deployment group is using the deployment configuration 'CodeDeployDefault.LambdaAllAtOnce'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentic ation enabled. The rule is NON_COMPL IANT if an Amazon Neptune cluster does not have IAM database authentic ation enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentic ation enabled. The rule is NON_COMPL IANT if an Amazon Neptune cluster does not have IAM database authentic ation enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.4 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentic ation enabled. The rule is NON_COMPL IANT if an Amazon Neptune cluster does not have IAM database authentic ation enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.5.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.6 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.6 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentic ation enabled. The rule is NON_COMPL IANT if an Amazon Neptune cluster does not have IAM database authentic ation enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentic ation enabled. The rule is NON_COMPL IANT if an Amazon Neptune cluster does not have IAM database authentic ation enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentic ation enabled. The rule is NON_COMPL IANT if an Amazon Neptune cluster does not have IAM database authentic ation enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.1 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.1 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | codebuild-project-envvar-awscred-check | Ensure that the project DOES NOT contain environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |
| 8.2.4 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.4 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.5 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.5 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |
| 8.2.6 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-imdsv2-check | Ensure that your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON_COMPLIANT if the HttpTokens is set to optional. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | autoscaling-launchconfig-requires-imdsv2 | Ensure that only IMDSv2 is enabled. This rule is NON_COMPLIANT if the Metadata version is not included in the launch configuration or if both Metadata V1 and V2 are enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.10.1 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |
| 8.3.10.1 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.10.1 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |
| 8.3.11 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.3.11 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | athena-workgroup-encrypted-at-rest | Ensure that an Amazon Athena workgroup is encrypted at rest. The rule is NON_COMPLIANT if encryption of data at rest is not enabled for an Athena workgroup. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | neptune-cluster-snapshot-encrypted | Ensure that an Amazon Neptune DB cluster has snapshots encrypted. The rule is NON_COMPLIANT if a Neptune cluster does not have snapshots encrypted. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | redshift-cluster-kms-enabled | Ensure that Amazon Redshift clusters are using a specified AWS Key Management Service (AWS KMS) key for encryptio n. The rule is COMPLIANT if encryption is enabled and the cluster is encrypted with the key provided in the kmsKeyArn parameter. The rule is NON_COMPL IANT if the cluster is not encrypted or encrypted with another key. |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | codebuild-project-s3-logs-encrypted | Ensure that an AWS CodeBuild project configured with Amazon S3 Logs has encryption enabled for its logs. The rule is NON_COMPLIANT if 'encryptionDisable d' is set to 'true' in a S3LogsConfig of a CodeBuild project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dms-redis-tls-enabled | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL encryption is not enabled. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | eks-secrets-encrypted | Ensure that Amazon Elastic Kubernetes Service clusters are configured to have Kubernetes secrets encrypted using AWS Key Management Service (KMS) keys. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | api-gw-cache-enabled-and-encrypted | Ensure that all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in an Amazon API Gateway stage is not configured to cache or the cache is not encrypted. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dynamodb-table-encrypted-kms | Ensure that Amazon DynamoDB table is encrypted with AWS Key Management Service (KMS). The rule is NON_COMPLIANT if Amazon DynamoDB table is not encrypted with AWS KMS. The rule is also NON_COMPLIANT if the encrypted AWS KMS key is not present in kmsKeyArns input parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | codebuild-project-envvar-awscred-check | Ensure that the project DOES NOT contain environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | eks-cluster-secrets-encrypted | Ensure that Amazon EKS clusters are not configured to have Kubernetes secrets encrypted using AWS KMS. The rule is NON_COMPLIANT if an EKS cluster does not have an encryptio nConfig resource or if encryptionConfig does not name secrets as a resource. |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | kinesis-stream-enc rypted | Ensure that Amazon Kinesis streams are encrypted at rest with server-side encryption. The rule is NON_COMPLIANT for a Kinesis stream if 'StreamEncryption' is not present. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | neptune-cluster-encrypted | Ensure that storage encryption is enabled for your Amazon Neptune DB clusters. The rule is NON_COMPLIANT if storage encryption is not enabled. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.5 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |
| 8.3.5 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.5 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |
| 8.3.7 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.7 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |
| 8.3.7 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.9 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |
| 8.3.9 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.9 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |
| 8.4.1 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |
| 8.4.2 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.4.3 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |
| 8.6.3 | Use of application and system accounts and associated authentication factors is strictly managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.6.3 | Use of application and system accounts and associated authentication factors is strictly managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |
| 8.6.3 | Use of application and system accounts and associated authentication factors is strictly managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifier (INCOMING_SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | emr-block-public-a ccess | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurit yGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGrou pRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| A1.2.3 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | security-account-information-provided | Ensure that you have provided security contact information for your AWS account contacts. The rule is NON_COMPLIANT if security contact information within the account is not provided. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A3.2.5.1 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-auto-sensitive-data-discovery-check | Ensure that automated sensitive data discovery is enabled for Amazon Macie. The rule is NON_COMPLIANT if automated sensitive data discovery is disabled. The rule is APPLICABLE for administrator accounts and NOT_APPLICABLE for member accounts. |
| A3.2.5.1 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-status-check | Ensure that Amazon Macie is enabled in your account per region. The rule is NON_COMPLIANT if the 'status' attribute is not set to 'ENABLED'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.2.5.2 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-auto-sensitive-data-discovery-check | Ensure that automated sensitive data discovery is enabled for Amazon Macie. The rule is NON_COMPLIANT if automated sensitive data discovery is disabled. The rule is APPLICABLE for administrator accounts and NOT_APPLICABLE for member accounts. |
| A3.2.5.2 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-status-check | Ensure that Amazon Macie is enabled in your account per region. The rule is NON_COMPLIANT if the 'status' attribute is not set to 'ENABLED'. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGroupRuleRanges. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

### Template

The template is available on GitHub: Operational Best Practices for PCI DSS 4.0 (Excluding global resource types).

## Operational Best Practices for PCI DSS 4.0 (Including global resource types)

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Payment Card Industry Data Security Standard (PCI DSS) 4.0 (Excluding global resource types) and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more PCI DSS controls. A PCI DSS control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.5 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | cloudfront-security-policy-check | Ensure that Amazon CloudFront distributions are using a minimum security policy and cipher suite of TLSv1.2 or greater for viewer connections. This rule is NON_COMPLIANT for a CloudFront distribution if the minimumProtocolVersion is below TLSv1.2_2018. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.5 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | cloudfront-sni-enabled | Ensure that Amazon CloudFront distributions are using a custom SSL certificate and are configured to use SNI to serve HTTPS requests. The rule is NON_COMPLIANT if a custom SSL certificate is associated but the SSL support method is a dedicated IP address. |
| 1.2.5 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | transfer-family-server-no-ftp | Ensure that a server created with AWS Transfer Family does not use FTP for endpoint connection. The rule is NON_COMPLIANT if the server protocol for endpoint connection is FTP-enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.5 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | cloudfront-no-deprecated-ssl-protocols | Ensure that CloudFront distributions are not using deprecated SSL protocols for HTTPS communication between CloudFront edge locations and custom origins. This rule is NON_COMPLIANT for a CloudFront distribution if any'OriginSslProtocols' includes'SSLv3'. |
| 1.2.5 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | cloudfront-traffic-to-origin-encrypted | Ensure that Amazon CloudFront distributions are encrypting traffic to custom origins. The rule is NON_COMPLIANT if'OriginProtocolPolicy' is'http-only' or if'OriginProtocolPolicy' is'match-viewer' and'ViewerProtocolPolicy' is'allow-all'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.5 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | cloudfront-viewer-policy-https | Ensure that your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the DefaultCacheBehavior or for the CacheBehaviors. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | rds-db-security-group-not-allowed | Ensure that the Amazon Relational Database Service (Amazon RDS) DB security groups is the default one. The rule is NON_COMPLIANT if there are any DB security groups that are not the default DB security group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | ec2-transit-gateway-auto-vpc-attach-disabled | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways do not have 'AutoAcceptSharedAttachments' enabled. The rule is NON_COMPLIANT for a Transit Gateway if 'AutoAcceptSharedAttachments' is set to 'enable'. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifie r (INCOMING _SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.2.8 | Network security controls (NSCs) are configured and maintained. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | rds-db-security-group-not-allowed | Ensure that the Amazon Relational Database Service (Amazon RDS) DB security groups is the default one. The rule is NON_COMPLIANT if there are any DB security groups that are not the default DB security group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | ec2-transit-gateway-auto-vpc-attach-disabled | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways do not have 'AutoAcceptSharedAttachments' enabled. The rule is NON_COMPLIANT for a Transit Gateway if 'AutoAcceptSharedAttachments' is set to 'enable'. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifie r (INCOMING _SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.3.1 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | rds-db-security-group-not-allowed | Ensure that the Amazon Relational Database Service (Amazon RDS) DB security groups is the default one. The rule is NON_COMPLIANT if there are any DB security groups that are not the default DB security group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | ec2-transit-gateway-auto-vpc-attach-disabled | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways do not have 'AutoAcceptSharedAttachments' enabled. The rule is NON_COMPLIANT for a Transit Gateway if 'AutoAcceptSharedAttachments' is set to 'enable'. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifier (INCOMING_SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.3.2 | Network access to and from the cardholder data environment is restricted. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 1.4.1 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.4.1 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.4.1 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | rds-db-security-group-not-allowed | Ensure that the Amazon Relational Database Service (Amazon RDS) DB security groups is the default one. The rule is NON_COMPLIANT if there are any DB security groups that are not the default DB security group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | ec2-transit-gateway-auto-vpc-attach-disabled | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways do not have 'AutoAcceptSharedAttachments' enabled. The rule is NON_COMPLIANT for a Transit Gateway if 'AutoAcceptSharedAttachments' is set to 'enable'. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifie r (INCOMING _SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | emr-block-public-a ccess | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurit yGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGrou pRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.4.2 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.3 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |
| 1.4.3 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.3 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | netfw-policy-default-action-full-packets | Ensure that an AWS Network Firewall policy is configured with a user defined default stateless action for full packets. This rule is NON_COMPLIANT if default stateless action for full packets does not match with user defined default stateless action. |
| 1.4.4 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.4 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | redshift-enhanced-vpc-routing-enabled | Ensure that Amazon Redshift clusters have 'enhancedVpcRouting' enabled. The rule is NON_COMPLIANT if 'enhancedVpcRouting' is not enabled or if the configuration.enhancedVpcRouting field is 'false'. |
| 1.4.4 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.4.5 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | ecs-task-definition-pid-mode-check | Ensure that ECSTaskDefinitions are configured to share a host's process namespace with its Amazon Elastic Container Service (Amazon ECS) containers. The rule is NON_COMPLIANT if the pidMode parameter is set to'host'. |
| 1.4.5 | Network connections between trusted and untrusted networks are controlled. (PCI-DSS-v4.0) | ec2-launch-template-public-ip-disabled | Ensure that Amazon EC2 Launch Templates are not set to assign public IP addresses to Network Interfaces. The rule is NON_COMPLIANT if the default version of an EC2 Launch Template has at least 1 Network Interface with 'AssociatePublicIpAddress' set to 'true'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | rds-db-security-group-not-allowed | Ensure that the Amazon Relational Database Service (Amazon RDS) DB security groups is the default one. The rule is NON_COMPLIANT if there are any DB security groups that are not the default DB security group. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | ec2-transit-gateway-auto-vpc-attach-disabled | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways do not have 'AutoAcceptSharedAttachments' enabled. The rule is NON_COMPLIANT for a Transit Gateway if 'AutoAcceptSharedAttachments' is set to 'enable'. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifie r (INCOMING _SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | emr-block-public-a ccess | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurit yGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGrou pRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 1.5.1 | Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.1 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.3 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.4 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.5 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.6 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.1.7 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.2.2 | Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.3.1 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGroupRuleRanges. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 10.3.2 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | aurora-resources-protected-by-backup-plan | Ensure that Amazon Aurora DB clusters are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon Relational Database Service (Amazon RDS) Database Cluster is not protected by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | db-instance-backup-enabled | Ensure that RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | dynamodb-in-backup-plan | Ensure that Amazon DynamoDB tables are present in AWS Backup Plans. The rule is NON_COMPLIANT if Amazon DynamoDB tables are not present in any AWS Backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | dynamodb-resources-protected-by-backup-plan | Ensure that Amazon DynamoDB tables are protected by a backup plan. The rule is NON_COMPLIANT if the DynamoDB Table is not covered by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ebs-in-backup-plan | Ensure that Amazon Elastic Block Store (Amazon EBS) volumes are added in backup plans of AWS Backup. The rule is NON_COMPLIANT if Amazon EBS volumes are not included in backup plans. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ebs-resources-protected-by-backup-plan | Ensure that Amazon Elastic Block Store (Amazon EBS) volumes are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon EBS volume is not covered by a backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | ec2-resources-protected-by-backup-plan | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) instances are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon EC2 instance is not covered by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | efs-in-backup-plan | Ensure that Amazon Elastic File System (Amazon EFS) file systems are added in the backup plans of AWS Backup. The rule is NON_COMPLIANT if EFS file systems are not included in the backup plans. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | efs-resources-protected-by-backup-plan | Ensure that Amazon Elastic File System (Amazon EFS) file systems are protected by a backup plan. The rule is NON_COMPLIANT if the EFS File System is not covered by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | elasticache-redis-cluster-automatic-backup-check | Check if the Amazon ElastiCache Redis clusters have automatic backup turned on. The rule is NON_COMPLIANT if the SnapshotRetentionLimit for Redis cluster is less than the SnapshotRetentionPeriod parameter. For example: If the parameter is 15 then the rule is non-compliant if the snapshotRetentionPeriod is between 0-15. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | fsx-resources-protected-by-backup-plan | Ensure that Amazon FSx File Systems are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon FSx File System is not covered by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | neptune-cluster-backup-retention-check | Ensure that an Amazon Neptune DB cluster retention period is set to specific number of days. The rule is NON_COMPLIANT if the retention period is less than the value specified by the parameter. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | rds-in-backup-plan | Ensure that Amazon Relational Database Service (Amazon RDS) databases are present in AWS Backup plans. The rule is NON_COMPLIANT if Amazon RDS databases are not included in any AWS Backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | rds-resources-protected-by-backup-plan | Ensure that Amazon Relational Database Service (Amazon RDS) instances are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon RDS Database instance is not covered by a backup plan. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | redshift-backup-enabled | Ensure that Amazon Redshift automated snapshots are enabled for clusters. The rule is NON_COMPLIANT if the value for automated SnapshotRetentionPeriod is greater than MaxRetentionPeriod or less than MinRetentionPeriod or the value is 0. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-resources-protected-by-backup-plan | Ensure that Amazon Simple Storage Service (Amazon S3) buckets are protected by a backup plan. The rule is NON_COMPLIANT if the Amazon S3 bucket is not covered by a backup plan. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | db-instance-backup-enabled | Ensure that RDS DB instances have backups enabled. Optionally, the rule checks the backup retention period and the backup window. |
| 10.3.3 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudfront-origin-access-identity-enabled | Ensure that CloudFront distribution with Amazon S3 Origin type has origin access identity (OAI) configured. The rule is NON_COMPLIANT if the CloudFront distribution is backed by S3 and any origin type is not OAI configured, or the origin is not an S3 bucket. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudfront-s3-origin-access-control-enabled | Ensure that an Amazon CloudFront distribution with an Amazon Simple Storage Service (Amazon S3) Origin type has origin access control (OAC) enabled. The rule is NON_COMPLIANT for CloudFront distributions with Amazon S3 origins that don't have OAC enabled. |
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-bucket-default-lock-enabled | Ensure that the S3 bucket has lock enabled, by default. The rule is NON_COMPLIANT if the lock is not enabled. |
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | s3-bucket-versioning-enabled | Ensure that versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.3.4 | Audit logs are protected from destruction and unauthorized modifications. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.4.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.1.1 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.4.2 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.4.3 | Audit logs are reviewed to identify anomalies or suspicious activity. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repositor y. |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | dynamodb-pitr-enab led | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 10.5.1 | Audit log history is retained and available for analysis. (PCI-DSS-v4.0) | cw-loggroup-retent ion-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPL IANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 10.6.3 | Time-synchronization mechanisms support consistent time settings across all systems. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudformation-stack-notification-check | Ensure that your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally ensure that specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.7.1 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudformation-stack-notification-check | Ensure that your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally ensure that specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |
| 10.7.2 | Failures of critical security control systems are detected, reported, and responded to promptly. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | cloudformation-stack-notification-check | Ensure that your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally ensure that specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications. |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| 11.5.2 | Network intrusions and unexpected file changes are detected and responded to. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | cloudformation-stack-notification-check | Ensure that your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally ensure that specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications. |
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| 11.6.1 | Unauthorized changes on payment pages are detected and responded to. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | cloudformation-stack-notification-check | Ensure that your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally ensure that specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications. |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 12.10.5 | Suspected and confirmed security incidents that could impact the CDE are responded to immediately. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| 12.4.2.1 | PCI DSS compliance is managed. (PCI-DSS-v4.0) | service-catalog-shared-within-organization | Ensure that AWS Service Catalog shares portfolios to an organization (a collection of AWS accounts treated as a single unit) when integration is enabled with AWS Organizations. The rule is NON_COMPLIANT if the `Type` value of a share is `ACCOUNT`. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.5 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-security-policy-check | Ensure that Amazon CloudFront distributions are using a minimum security policy and cipher suite of TLSv1.2 or greater for viewer connections. This rule is NON_COMPLIANT for a CloudFront distribution if the minimumProtocolVersion is below TLSv1.2_2018. |
| 2.2.5 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-sni-enabled | Ensure that Amazon CloudFront distributions are using a custom SSL certificate and are configured to use SNI to serve HTTPS requests. The rule is NON_COMPLIANT if a custom SSL certificate is associated but the SSL support method is a dedicated IP address. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.5 | System components are configured and managed securely. (PCI-DSS-v4.0) | transfer-family-server-no-ftp | Ensure that a server created with AWS Transfer Family does not use FTP for endpoint connection. The rule is NON_COMPLIANT if the server protocol for endpoint connection is FTP-enabled. |
| 2.2.5 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-no-deprecated-ssl-protocols | Ensure that CloudFront distributions are not using deprecated SSL protocols for HTTPS communication between CloudFront edge locations and custom origins. This rule is NON_COMPLIANT for a CloudFront distribution if any'OriginSslProtocols' includes'SSLv3'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.5 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-traffic-to-origin-encrypted | Ensure that Amazon CloudFront distributions are encrypting traffic to custom origins. The rule is NON_COMPLIANT if'OriginProtocolPolicy' is'http-only' or if'OriginProtocolPolicy' is'match-viewer' and'ViewerProtocolPolicy' is'allow-all'. |
| 2.2.5 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-viewer-policy-https | Ensure that your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the DefaultCacheBehavior or for the CacheBehaviors. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | dms-redis-tls-enabled | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL encryption is not enabled. |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-no-deprecated-ssl-protocols | Ensure that CloudFront distributions are not using deprecated SSL protocols for HTTPS communication between CloudFront edge locations and custom origins. This rule is NON_COMPLIANT for a CloudFront distribution if any'OriginSslProtocols' includes'SSLv3'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-traffic-to-origin-encrypted | Ensure that Amazon CloudFront distributions are encrypting traffic to custom origins. The rule is NON_COMPLIANT if'OriginProtocolPolicy' is'http-only' or if'OriginProtocolPolicy' is'match-viewer' and'ViewerProtocolPolicy' is'allow-all'. |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | cloudfront-viewer-policy-https | Ensure that your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the DefaultCacheBehavior or for the CacheBehaviors. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | dax-tls-endpoint-encryption | Ensure that your Amazon DynamoDB Accelerator (DAX) cluster has ClusterEndpointEncryptionType set to TLS. The rule is NON_COMPLIANT if a DAX cluster is not encrypted by transport layer security (TLS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |
| 2.2.7 | System components are configured and managed securely. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repositor y. |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 3.2.1 | Storage of account data is kept to a minimum. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPL IANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.1.1 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 3.3.1.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |
| 3.3.2 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ec2-volume-inuse-check | Ensure that EBS volumes are attached to EC2 instances. Optionally ensure that EBS volumes are marked for deletion when an instance is terminated. |
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | ecr-private-lifecycle-policy-configured | Ensure that a private Amazon Elastic Container Registry (ECR) repository has at least one lifecycle policy configured. The rule is NON_COMPLIANT if no lifecycle policy is configured for the ECR private repository. |
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | dynamodb-pitr-enabled | Ensure that point-in-time recovery (PITR) is enabled for Amazon DynamoDB tables. The rule is NON_COMPLIANT if PITR is not enabled for DynamoDB tables. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.3.3 | Sensitive authentication data (SAD) is not stored after authorization. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | athena-workgroup-encrypted-at-rest | Ensure that an Amazon Athena workgroup is encrypted at rest. The rule is NON_COMPLIANT if encryption of data at rest is not enabled for an Athena workgroup. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | neptune-cluster-snapshot-encrypted | Ensure that an Amazon Neptune DB cluster has snapshots encrypted. The rule is NON_COMPLIANT if a Neptune cluster does not have snapshots encrypted. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | redshift-cluster-kms-enabled | Ensure that Amazon Redshift clusters are using a specified AWS Key Management Service (AWS KMS) key for encryptio n. The rule is COMPLIANT if encryption is enabled and the cluster is encrypted with the key provided in the kmsKeyArn parameter. The rule is NON_COMPL IANT if the cluster is not encrypted or encrypted with another key. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | codebuild-project-artifact-encryption | Ensure that an AWS CodeBuild project has encryption enabled for all of its artifacts. The rule is NON_COMPLIANT if 'encryptionDisabled' is set to 'true' for any primary or secondary (if present) artifact configurations. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | codebuild-project-s3-logs-encrypted | Ensure that an AWS CodeBuild project configured with Amazon S3 Logs has encryption enabled for its logs. The rule is NON_COMPLIANT if'encryptionDisabled' is set to'true' in a S3LogsConfig of a CodeBuild project. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | dax-encryption-enabled | Ensure that Amazon DynamoDB Accelerator (DAX) clusters are encrypted. The rule is NON_COMPLIANT if a DAX cluster is not encrypted. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | eks-secrets-encrypted | Ensure that Amazon Elastic Kubernetes Service clusters are configured to have Kubernetes secrets encrypted using AWS Key Management Service (KMS) keys. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | api-gw-cache-enabled-and-encrypted | Ensure that all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in an Amazon API Gateway stage is not configured to cache or the cache is not encrypted. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | docdb-cluster-encrypted | Ensure that storage encryption is enabled for your Amazon DocumentDB (with MongoDB compatibility) clusters. The rule is NON_COMPLIANT if storage encryption is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | dynamodb-table-encrypted-kms | Ensure that Amazon DynamoDB table is encrypted with AWS Key Management Service (KMS). The rule is NON_COMPLIANT if Amazon DynamoDB table is not encrypted with AWS KMS. The rule is also NON_COMPLIANT if the encrypted AWS KMS key is not present in kmsKeyArns input parameter. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | dynamodb-table-encryption-enabled | Ensure that the Amazon DynamoDB tables are encrypted and checks their status. The rule is COMPLIANT if the status is enabled or enabling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | codebuild-project-envvar-awscred-check | Ensure that the project DOES NOT contain environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | eks-cluster-secrets-encrypted | Ensure that Amazon EKS clusters are not configured to have Kubernetes secrets encrypted using AWS KMS. The rule is NON_COMPLIANT if an EKS cluster does not have an encryptionConfig resource or if encryptionConfig does not name secrets as a resource. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | kinesis-stream-encrypted | Ensure that Amazon Kinesis streams are encrypted at rest with server-side encryption. The rule is NON_COMPLIANT for a Kinesis stream if 'StreamEncryption' is not present. |
| 3.5.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | neptune-cluster-encrypted | Ensure that storage encryption is enabled for your Amazon Neptune DB clusters. The rule is NON_COMPLIANT if storage encryption is not enabled. |
| 3.5.1.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |
| 3.5.1.1 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in PermittedPublicSecurityGroupRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| 3.5.1.3 | Primary account number (PAN) is secured wherever it is stored. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.6.1 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.6.1.2 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1.2 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |
| 3.6.1.2 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1.3 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.6.1.3 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1.3 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.6.1.4 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.6.1.4 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |
| 3.6.1.4 | Cryptographic keys used to protect stored account data are secured. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.1 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-certificate-rsa-check | Ensure that RSA certificates managed by AWS Certificate Manager (ACM) have a key length of at least '2048' bits.The rule is NON_COMPL IANT if the minimum key length is less than 2048 bits. |
| 3.7.1 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.7.1 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associate d with an Amazon CloudFront distribut ion is not the default SSL certificate. The rule is NON_COMPL IANT if a CloudFront distribution uses the default SSL certifica te. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.1 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.7.2 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.2 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associate d with an Amazon CloudFront distribut ion is not the default SSL certificate. The rule is NON_COMPL IANT if a CloudFront distribution uses the default SSL certifica te. |
| 3.7.2 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.4 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.7.4 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associate d with an Amazon CloudFront distribut ion is not the default SSL certificate. The rule is NON_COMPL IANT if a CloudFront distribution uses the default SSL certifica te. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.4 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 3.7.6 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.6 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associate d with an Amazon CloudFront distribut ion is not the default SSL certificate. The rule is NON_COMPL IANT if a CloudFront distribution uses the default SSL certifica te. |
| 3.7.6 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.7 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | acm-pca-root-ca-di sabled | Ensure that AWS Private Certifica te Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 3.7.7 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associate d with an Amazon CloudFront distribut ion is not the default SSL certificate. The rule is NON_COMPL IANT if a CloudFront distribution uses the default SSL certifica te. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.7.7 | Where cryptography is used to protect stored account data, key managemen t processes and procedures covering all aspects of the key lifecycle are defined and implemented. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-redis-tls-enab led | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPL IANT if TLS/SSL encryption is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-no-deprecated-ssl-protocols | Ensure that CloudFront distributions are not using deprecated SSL protocols for HTTPS communication between CloudFront edge locations and custom origins. This rule is NON_COMPLIANT for a CloudFront distribution if any'OriginSslProtocols' includes'SSLv3'. |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-traffic-to-origin-encrypted | Ensure that Amazon CloudFront distributions are encrypting traffic to custom origins. The rule is NON_COMPLIANT if'OriginProtocolPolicy' is'http-only' or if'OriginProtocolPolicy' is'match-viewer' and'ViewerProtocolPolicy' is'allow-all'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-viewer-policy-https | Ensure that your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the DefaultCacheBehavior or for the CacheBehaviors. |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dax-tls-endpoint-encryption | Ensure that your Amazon DynamoDB Accelerator (DAX) cluster has ClusterEndpointEncryptionType set to TLS. The rule is NON_COMPLIANT if a DAX cluster is not encrypted by transport layer security (TLS). |
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.2.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | acm-pca-root-ca-disabled | Ensure that AWS Private Certificate Authority (AWS Private CA) has a root CA that is disabled. The rule is NON_COMPLIANT for root CAs with status that is not DISABLED. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-redis-tls-enabled | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL encryption is not enabled. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-no-deprecated-ssl-protocols | Ensure that CloudFront distributions are not using deprecated SSL protocols for HTTPS communication between CloudFront edge locations and custom origins. This rule is NON_COMPLIANT for a CloudFront distribution if any'OriginSslProtocols' includes'SSLv3'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-traffic-to-origin-encrypted | Ensure that Amazon CloudFront distributions are encrypting traffic to custom origins. The rule is NON_COMPLIANT if'OriginProtocolPolicy' is'http-only' or if'OriginProtocolPolicy' is'match-viewer' and'ViewerProtocolPolicy' is'allow-all'. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | cloudfront-viewer-policy-https | Ensure that your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the DefaultCacheBehavior or for the CacheBehaviors. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dax-tls-endpoint-e ncryption | Ensure that your Amazon DynamoDB Accelerator (DAX) cluster has ClusterEn dpointEncryptionTy pe set to TLS. The rule is NON_COMPL IANT if a DAX cluster is not encrypted by transport layer security (TLS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |
| 4.2.1.1 | PAN is protected with strong cryptography during transmission. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 5.3.4 | Anti-malware mechanisms and processes are active, maintained, and monitored. (PCI-DSS-v4.0) | cw-loggroup-retention-period-check | Ensure that an Amazon CloudWatch LogGroup retention period is set to greater than 365 days or else a specified retention period. The rule is NON_COMPLIANT if the retention period is less than MinRetentionTime, if specified, or else 365 days. |
| 6.3.3 | Security vulnerabilities are identified and addressed. (PCI-DSS-v4.0) | lambda-function-settings-check | Ensure that the AWS Lambda function settings for runtime, role, timeout, and memory size match the expected values. The rule ignores functions with the 'Image' package type and functions with runtime set to 'OS-only Runtime'. The rule is NON_COMPLIANT if the Lambda function settings do not match the expected values. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3.3 | Security vulnerabilities are identified and addressed. (PCI-DSS-v4.0) | eks-cluster-oldest-supported-version | Ensure that an Amazon Elastic Kubernetes Service (EKS) cluster is not running the oldest supported version. The rule is NON_COMPLIANT if an EKS cluster is running oldest supported version (equal to the parameter 'oldestVersionSupported'). |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-webacl-not-empty | Ensure that a WAFv2 Web ACL contains any WAF rules or WAF rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rules or WAF rule groups. |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-rulegroup-not-empty | Ensure that WAFv2 Rule Groups contain rules. The rule is NON_COMPLIANT if there are no rules in a WAFv2 Rule Group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.4.1 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-webacl-not-empty | Ensure that a WAFv2 Web ACL contains any WAF rules or WAF rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rules or WAF rule groups. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | wafv2-rulegroup-not-empty | Ensure that WAFv2 Rule Groups contain rules. The rule is NON_COMPLIANT if there are no rules in a WAFv2 Rule Group. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |
| 6.4.2 | Public-facing web applications are protected against attacks. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| 6.5.5 | Changes to all system components are managed securely. (PCI-DSS-v4.0) | codedeploy-lambda-allatonce-traffic-shift-disabled | Ensure that the deployment group for Lambda Compute Platform is not using the default deployment configuration. The rule is NON_COMPLIANT if the deployment group is using the deployment configuration 'CodeDeployDefault.LambdaAllAtOnce'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.5.5 | Changes to all system components are managed securely. (PCI-DSS-v4.0) | codepipeline-deployment-count-check | Ensure that the first deployment stage of AWS CodePipeline performs at least one deployment. This is to monitor continuous deployment activity, ensuring regular updates and identifying inactive or underutilized pipelines, which can signal issues in the development or deployment process. Optionally ensure that each of the subsequent remaining stages deploy to more than the specified number of deployments (deploymentLimit). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.5.6 | Changes to all system components are managed securely. (PCI-DSS-v4.0) | codedeploy-lambda-allatonce-traffic-shift-disabled | Ensure that the deployment group for Lambda Compute Platform is not using the default deployment configuration. The rule is NON_COMPLIANT if the deployment group is using the deployment configuration 'CodeDeployDefault.LambdaAllAtOnce'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.5.6 | Changes to all system components are managed securely. (PCI-DSS-v4.0) | codepipeline-deployment-count-check | Ensure that the first deployment stage of AWS CodePipeline performs at least one deployment. This is to monitor continuous deployment activity, ensuring regular updates and identifying inactive or underutilized pipelines, which can signal issues in the development or deployment process. Optionally ensure that each of the subsequent remaining stages deploy to more than the specified number of deployments (deploymentLimit). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.2 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |
| 7.2.4 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.5 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |
| 7.2.5.1 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.6 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.2.6 | Access to system components and data is appropriately defined and assigned. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.1 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.2 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissio ns than the control Amazon S3 bucket policy that you provide. |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 7.3.3 | Access to system components and data is managed via an access control system(s). (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |
| 8.2.1 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.1 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | codebuild-project-envvar-awscred-check | Ensure that the project DOES NOT contain environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.2 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |
| 8.2.4 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.4 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.2.5 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.2.5 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |
| 8.2.6 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.7 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-imdsv2-check | Ensure that your Amazon Elastic Compute Cloud (Amazon EC2) instance metadata version is configured with Instance Metadata Service Version 2 (IMDSv2). The rule is NON_COMPLIANT if the HttpTokens is set to optional. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | autoscaling-launchconfig-requires-imdsv2 | Ensure that only IMDSv2 is enabled. This rule is NON_COMPLIANT if the Metadata version is not included in the launch configuration or if both Metadata V1 and V2 are enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.2.8 | User identification and related accounts for users and administrators are strictly managed throughout an accounts lifecycle. (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |
| 8.3.10.1 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.10.1 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |
| 8.3.10.1 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.11 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |
| 8.3.11 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | ec2-no-amazon-key-pair | Ensure that running Amazon Elastic Compute Cloud (EC2) instances are not launched using amazon key pairs. The rule is NON_COMPLIANT if a running EC2 instance is launched with a key pair. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | athena-workgroup-encrypted-at-rest | Ensure that an Amazon Athena workgroup is encrypted at rest. The rule is NON_COMPLIANT if encryption of data at rest is not enabled for an Athena workgroup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | neptune-cluster-snapshot-encrypted | Ensure that an Amazon Neptune DB cluster has snapshots encrypted. The rule is NON_COMPLIANT if a Neptune cluster does not have snapshots encrypted. |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | redshift-cluster-kms-enabled | Ensure that Amazon Redshift clusters are using a specified AWS Key Management Service (AWS KMS) key for encryptio n. The rule is COMPLIANT if encryption is enabled and the cluster is encrypted with the key provided in the kmsKeyArn parameter. The rule is NON_COMPL IANT if the cluster is not encrypted or encrypted with another key. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | codebuild-project-artifact-encryption | Ensure that an AWS CodeBuild project has encryption enabled for all of its artifacts. The rule is NON_COMPLIANT if 'encryptionDisabled' is set to 'true' for any primary or secondary (if present) artifact configurations. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | codebuild-project-s3-logs-encrypted | Ensure that an AWS CodeBuild project configured with Amazon S3 Logs has encryption enabled for its logs. The rule is NON_COMPLIANT if'encryptionDisabled' is set to'true' in a S3LogsConfig of a CodeBuild project. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dax-encryption-enabled | Ensure that Amazon DynamoDB Accelerator (DAX) clusters are encrypted. The rule is NON_COMPLIANT if a DAX cluster is not encrypted. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dms-redis-tls-enabled | Ensure that AWS Database Migration Service (AWS DMS) endpoints for Redis data stores are enabled for TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL encryption is not enabled. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | eks-secrets-encrypted | Ensure that Amazon Elastic Kubernetes Service clusters are configured to have Kubernetes secrets encrypted using AWS Key Management Service (KMS) keys. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | api-gw-cache-enabled-and-encrypted | Ensure that all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in an Amazon API Gateway stage is not configured to cache or the cache is not encrypted. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | docdb-cluster-encrypted | Ensure that storage encryption is enabled for your Amazon DocumentDB (with MongoDB compatibility) clusters. The rule is NON_COMPLIANT if storage encryption is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dynamodb-table-encrypted-kms | Ensure that Amazon DynamoDB table is encrypted with AWS Key Management Service (KMS). The rule is NON_COMPLIANT if Amazon DynamoDB table is not encrypted with AWS KMS. The rule is also NON_COMPLIANT if the encrypted AWS KMS key is not present in kmsKeyArns input parameter. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dynamodb-table-encryption-enabled | Ensure that the Amazon DynamoDB tables are encrypted and checks their status. The rule is COMPLIANT if the status is enabled or enabling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | cloudfront-no-deprecated-ssl-protocols | Ensure that CloudFront distributions are not using deprecated SSL protocols for HTTPS communication between CloudFront edge locations and custom origins. This rule is NON_COMPLIANT for a CloudFront distribution if any'OriginSslProtocols' includes'SSLv3'. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | cloudfront-traffic-to-origin-encrypted | Ensure that Amazon CloudFront distributions are encrypting traffic to custom origins. The rule is NON_COMPLIANT if'OriginProtocolPolicy' is'http-only' or if'OriginProtocolPolicy' is'match-viewer' and'ViewerProtocolPolicy' is'allow-all'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | cloudfront-viewer-policy-https | Ensure that your Amazon CloudFront distributions use HTTPS (directly or via a redirection). The rule is NON_COMPLIANT if the value of ViewerProtocolPolicy is set to 'allow-all' for the DefaultCacheBehavior or for the CacheBehaviors. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | codebuild-project-envvar-awscred-check | Ensure that the project DOES NOT contain environment variables AWS_ACCESS_KEY_ID and AWS_SECRET_ACCESS_KEY. The rule is NON_COMPLIANT when the project environment variables contains plaintext credentials. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certificate Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Application Load Balancers and Network Load Balancers. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dax-tls-endpoint-encryption | Ensure that your Amazon DynamoDB Accelerator (DAX) cluster has ClusterEndpointEncryptionType set to TLS. The rule is NON_COMPLIANT if a DAX cluster is not encrypted by transport layer security (TLS). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | eks-cluster-secrets-encrypted | Ensure that Amazon EKS clusters are not configured to have Kubernetes secrets encrypted using AWS KMS. The rule is NON_COMPLIANT if an EKS cluster does not have an encryptio nConfig resource or if encryptionConfig does not name secrets as a resource. |
| 8.3.2 | Strong authentic ation for users and administrators is established and managed. (PCI-DSS-v4.0) | kinesis-stream-enc rypted | Ensure that Amazon Kinesis streams are encrypted at rest with server-side encryption. The rule is NON_COMPLIANT for a Kinesis stream if 'StreamEncryption' is not present. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | msk-in-cluster-node-require-tls | Ensure that an Amazon MSK cluster enforces encryption in transit using HTTPS (TLS) with the broker nodes of the cluster. The rule is NON_COMPLIANT if plain text communication is enabled for in-cluster broker node connections. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | neptune-cluster-encrypted | Ensure that storage encryption is enabled for your Amazon Neptune DB clusters. The rule is NON_COMPLIANT if storage encryption is not enabled. |
| 8.3.2 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | dms-endpoint-ssl-configured | Ensure that AWS Database Migration Service (AWS DMS) endpoints are configured with an SSL connection. The rule is NON_COMPLIANT if AWS DMS does not have an SSL connection configured. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | s3-bucket-blacklisted-actions-prohibited | Ensure that an Amazon Simple Storage Service (Amazon S3) bucket policy does not allow blocklisted bucket-level and object-level actions on resources in the bucket for principals from other AWS accounts. For example, the rule checks that the Amazon S3 bucket policy does not allow another AWS account to perform any s3:GetBucket* actions and s3:DeleteObject on any object in the bucket. The rule is NON_COMPLIANT if any blocklisted actions are allowed by the Amazon S3 bucket policy. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | s3-bucket-policy-not-more-permissive | Ensure that your Amazon Simple Storage Service (S3) bucket policies do not allow other inter-account permissions than the control Amazon S3 bucket policy that you provide. |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | shield-drt-access | Ensure that the Shield Response Team (SRT) can access your AWS account. The rule is NON_COMPLIANT if AWS Shield Advanced is enabled but the role for SRT access is not configured. |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | iam-policy-in-use | Ensure that an IAM policy ARN is attached to an IAM user, or a group with one or more IAM users, or an IAM role with one or more trusted entity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | neptune-cluster-iam-database-authentication | Ensure that an Amazon Neptune cluster has AWS Identity and Access Management (IAM) database authentication enabled. The rule is NON_COMPLIANT if an Amazon Neptune cluster does not have IAM database authentication enabled. |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | rds-cluster-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) cluster has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS Cluster does not have IAM authentication enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | ec2-instance-profile-attached | Ensure that an EC2 instance has an AWS Identity and Access Management (IAM) profile attached to it. The rule is NON_COMPLIANT if no IAM profile is attached to the EC2 instance. |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.4 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | rds-instance-iam-authentication-enabled | Ensure that an Amazon Relational Database Service (Amazon RDS) instance has AWS Identity and Access Management (IAM) authentication enabled. The rule is NON_COMPLIANT if an Amazon RDS instance does not have IAM authentication enabled. |
| 8.3.5 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.5 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |
| 8.3.5 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.7 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |
| 8.3.7 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.7 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |
| 8.3.9 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccessKeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.3.9 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |
| 8.3.9 | Strong authentication for users and administrators is established and managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.4.1 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |
| 8.4.2 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |
| 8.4.3 | Multi-factor authentication (MFA) is implemented to secure access into the CDE. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.6.3 | Use of application and system accounts and associated authentication factors is strictly managed. (PCI-DSS-v4.0) | access-keys-rotated | Ensure that active IAM access keys are rotated (changed) within the number of days specified in maxAccess KeyAge. The rule is NON_COMPLIANT if access keys are not rotated within the specified time period. The default value is 90 days. |
| 8.6.3 | Use of application and system accounts and associated authentication factors is strictly managed. (PCI-DSS-v4.0) | secretsmanager-scheduled-rotation-success-check | Ensure that AWS Secrets Manager secrets rotated successfully according to the rotation schedule. Secrets Manager calculates the date the rotation should happen. The rule is NON_COMPLIANT if the date passes and the secret isn't rotated. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.6.3 | Use of application and system accounts and associated authentication factors is strictly managed. (PCI-DSS-v4.0) | secretsmanager-secret-periodic-rotation | Ensure that AWS Secrets Manager secrets have been rotated in the past specified number of days. The rule is NON_COMPLIANT if a secret has not been rotated for more than maxDaysSinceRotation number of days. The default value is 90 days. |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGroupRuleRanges. |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| A1.1.2 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | api-gw-endpoint-type-check | Ensure that Amazon API Gateway APIs are of the type specified in the rule parameter 'endpointConfigurationType'. The rule returns NON_COMPLIANT if the REST API does not match the endpoint type configured in the rule parameter. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | cloudfront-associated-with-waf | Ensure that Amazon CloudFront distributions are associated with either web application firewall (WAF) or WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT if a CloudFront distribution is not associated with a WAF web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | cloudfront-custom-ssl-certificate | Ensure that the certificate associated with an Amazon CloudFront distribution is not the default SSL certificate. The rule is NON_COMPLIANT if a CloudFront distribution uses the default SSL certificate. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | netfw-policy-default-action-fragment-packets | Ensure that an AWS Network Firewall policy is configured with a user defined stateless default action for fragmented packets. The rule is NON_COMPLIANT if stateless default action for fragmented packets does not match with user defined default action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | rds-db-security-group-not-allowed | Ensure that the Amazon Relational Database Service (Amazon RDS) DB security groups is the default one. The rule is NON_COMPLIANT if there are any DB security groups that are not the default DB security group. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | ec2-transit-gateway-auto-vpc-attach-disabled | Ensure that Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways do not have 'AutoAcceptSharedAttachments' enabled. The rule is NON_COMPLIANT for a Transit Gateway if 'AutoAcceptSharedAttachments' is set to 'enable'. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | eks-endpoint-no-public-access | Ensure that the Amazon Elastic Kubernetes Service (Amazon EKS) endpoint is not publicly accessible. The rule is NON_COMPLIANT if the endpoint is publicly accessible. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | restricted-ssh | Note: For this rule, the rule identifie r (INCOMING _SSH_DISABLED) and rule name (restricted-ssh) are different. Ensure that the incoming SSH traffic for the security groups is accessible. The rule is COMPLIANT if the IP addresses of the incoming SSH traffic in the security groups are restricted (CIDR other than 0.0.0.0/0 or ::/0). Otherwise, NON_COMPLIANT. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | appsync-associated-with-waf | Ensure that AWS AppSync APIs are associated with AWS WAFv2 web access control lists (ACLs). The rule is NON_COMPLIANT for an AWS AppSync API if it is not associated with a web ACL. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | codebuild-project-source-repo-url-check | Ensure that the Bitbucket source repository URL DOES NOT contain sign-in credentials or not. The rule is NON_COMPLIANT if the URL contains any sign-in information and COMPLIANT if it doesn't. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | elb-acm-certificate-required | Ensure that the Classic Load Balancers use SSL certificates provided by AWS Certifica te Manager. To use this rule, use an SSL or HTTPS listener with your Classic Load Balancer. Note - this rule is only applicable to Classic Load Balancers. This rule does not check Applicati on Load Balancers and Network Load Balancers. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | emr-block-public-a ccess | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurit yGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGrou pRuleRanges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | nacl-no-unrestricted-ssh-rdp | Ensure that default ports for SSH/RDP ingress traffic for network access control lists (NACLs) are restricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source TCP or UDP CIDR block for ports 22 or 3389. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | waf-global-webacl-not-empty | Ensure that a WAF Global Web ACL contains some WAF rules or rule groups. This rule is NON_COMPLIANT if a Web ACL does not contain any WAF rule or rule group. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | waf-global-rulegroup-not-empty | Ensure that an AWS WAF Classic rule group contains some rules. The rule is NON_COMPLIANT if there are no rules present within a rule group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | waf-global-rule-not-empty | Ensure that an AWS WAF global rule contains some conditions. The rule is NON_COMPLIANT if no conditions are present within the WAF global rule. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | ec2-client-vpn-not-authorize-all | Ensure that the AWS Client VPN authorization rules does not authorize connection access for all clients. The rule is NON_COMPLIANT if 'AccessAll' is present and set to true. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | internet-gateway-authorized-vpc-only | Ensure that internet gateways are attached to an authorized virtual private cloud (Amazon VPC). The rule is NON_COMPLIANT if internet gateways are attached to an unauthorized VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| A1.1.3 | Multi-tenant service providers protect and separate all customer environments and data. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | api-gwv2-access-logs-enabled | Ensure that Amazon API Gateway V2 stages have access logging enabled. The rule is NON_COMPLIANT if 'accessLogSettings' is not present in Stage configuration. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | cloudfront-accesslogs-enabled | Ensure that Amazon CloudFront distributions are configured to deliver access logs to an Amazon S3 bucket. The rule is NON_COMPLIANT if a CloudFront distribution does not have logging configured. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | cloudtrail-security-trail-enabled | Ensure that there is at least one AWS CloudTrail trail defined with security best practices. This rule is COMPLIANT if there is at least one trail that meets all of the following: |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | neptune-cluster-cloudwatch-log-export-enabled | Ensure that an Amazon Neptune cluster has CloudWatch log export enabled for audit logs. The rule is NON_COMPLIANT if a Neptune cluster does not have CloudWatch log export enabled for audit logs. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | ecs-task-definition-log-configuration | Ensure that logConfiguration is set on active ECS Task Definitions. This rule is NON_COMPLIANT if an active ECSTaskDefinition does not have the logConfiguration resource defined or the value for logConfiguration is null in at least one container definition. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | cloudtrail-enabled | Note: For this rule, the rule identifier (CLOUD_TRAIL_ENABLED) and rule name (cloudtrail-enabled) are different. Ensure that an AWS CloudTrail trail is enabled in your AWS account. The rule is NON_COMPLIANT if a trail is not enabled. Optionally, the rule checks a specific S3 bucket, Amazon Simple Notification Service (Amazon SNS) topic, and CloudWatch log group. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | multi-region-cloudtrail-enabled | Note: for this rule, the rule identifier (MULTI_REGION_CLOUD_TRAIL_ENABLED) and rule name (multi-region-cloudtrail-enabled) are different. Ensure that there is at least one multi-region AWS CloudTrail. The rule is NON_COMPLIANT if the trails do not match input parameters. The rule is NON_COMPLIANT if the ExcludeManagementEventSources field is not empty or if AWS CloudTrail is configured to exclude management events such as AWS KMS events or Amazon RDS Data API events. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | appsync-logging-enabled | Ensure that an AWS AppSync API has logging enabled. The rule is NON_COMPLIANT if logging is not enabled, or 'fieldLogLevel' is neither ERROR nor ALL. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | waf-classic-logging-enabled | Ensure that logging is enabled on AWS WAF classic global web access control lists (web ACLs). The rule is NON_COMPLIANT for a global web ACL, if it does not have logging enabled. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | mq-cloudwatch-audit-logging-enabled | Ensure that Amazon MQ brokers have Amazon CloudWatch audit logging enabled. The rule is NON_COMPLIANT if a broker does not have audit logging enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | mq-cloudwatch-audit-log-enabled | Ensure that an Amazon MQ broker has CloudWatch audit logging enabled. The rule is NON_COMPLIANT if the broker does not have audit logging enabled. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | eks-cluster-logging-enabled | Ensure that an Amazon Elastic Kubernetes Service (Amazon EKS) cluster is configured with logging enabled. The rule is NON_COMPLIANT if logging for Amazon EKS clusters is not enabled for all log types. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | elastic-beanstalk-logs-to-cloudwatch | Ensure that AWS Elastic Beanstalk environments are configured to send logs to Amazon CloudWatch Logs. The rule is NON_COMPLIANT if the value of `StreamLogs` is false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | step-functions-state-machine-logging-enabled | Ensure that AWS Step Functions machine has logging enabled. The rule is NON_COMPLIANT if a state machine does not have logging enabled or the logging configuration is not at the minimum level provided. |
| A1.2.1 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | netfw-logging-enabled | Ensure that AWS Network Firewall firewalls have logging enabled. The rule is NON_COMPLIANT if a logging type is not configured. You can specify which logging type you want the rule to check. |
| A1.2.3 | Multi-tenant service providers facilitate logging and incident response for all customers. (PCI-DSS-v4.0) | security-account-information-provided | Ensure that you have provided security contact information for your AWS account contacts. The rule is NON_COMPLIANT if security contact information within the account is not provided. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.2.5.1 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-auto-sensitive-data-discovery-check | Ensure that automated sensitive data discovery is enabled for Amazon Macie. The rule is NON_COMPLIANT if automated sensitive data discovery is disabled. The rule is APPLICABLE for administrator accounts and NOT_APPLICABLE for member accounts. |
| A3.2.5.1 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-status-check | Ensure that Amazon Macie is enabled in your account per region. The rule is NON_COMPLIANT if the 'status' attribute is not set to 'ENABLED'. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.2.5.2 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-auto-sensitive-data-discovery-check | Ensure that automated sensitive data discovery is enabled for Amazon Macie. The rule is NON_COMPLIANT if automated sensitive data discovery is disabled. The rule is APPLICABLE for administrator accounts and NOT_APPLICABLE for member accounts. |
| A3.2.5.2 | PCI DSS scope is documented and validated. (PCI-DSS-v4.0) | macie-status-check | Ensure that Amazon Macie is enabled in your account per region. The rule is NON_COMPLIANT if the 'status' attribute is not set to 'ENABLED'. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudformation-stack-notification-check | Ensure that your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally ensure that specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.3.1 | PCI DSS is incorporated into business-as-usual (BAU) activities. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | neptune-cluster-snapshot-public-prohibited | Ensure that an Amazon Neptune manual DB cluster snapshot is not public. The rule is NON_COMPLIANT if any existing and new Neptune cluster snapshot is public. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | docdb-cluster-snapshot-public-prohibited | Ensure that Amazon DocumentDB manual cluster snapshots are not public. The rule is NON_COMPLIANT if any Amazon DocumentDB manual cluster snapshots are public. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | backup-recovery-point-manual-deletion-disabled | Ensure that a backup vault has an attached resource-based policy which prevents deletion of recovery points. The rule is NON_COMPLIANT if the Backup Vault does not have resource-based policies or has policies without a suitable 'Deny' statement (statement with backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, and backup:PutBackupVaultAccessPolicy permissions). |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | emr-block-public-access | Ensure that an account with Amazon EMR has block public access settings enabled. The rule is NON_COMPLIANT if BlockPublicSecurityGroupRules is false, or if true, ports other than Port 22 are listed in Permitted PublicSecurityGroupRuleRanges. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | secretsmanager-secret-unused | Ensure that AWS Secrets Manager secrets have been accessed within a specified number of days. The rule is NON_COMPLIANT if a secret has not been accessed in 'unusedForDays' number of days. The default value is 90 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | s3-access-point-public-access-blocks | Ensure that Amazon S3 access points have block public access settings enabled. The rule is NON_COMPLIANT if block public access settings are not enabled for S3 access points. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | s3-account-level-public-access-blocks | Ensure that the required public access block settings are configured from account level. The rule is only NON_COMPLIANT when the fields set below do not match the corresponding fields in the configuration item. |
| A3.4.1 | Logical access to the cardholder data environment is controlled and managed. (PCI-DSS-v4.0) | s3-bucket-mfa-delete-enabled | Ensure that MFA Delete is enabled in the Amazon Simple Storage Service (Amazon S3) bucket versioning configuration. The rule is NON_COMPLIANT if MFA Delete is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | api-gw-xray-enabled | Ensure that AWS X-Ray tracing is enabled on Amazon API Gateway REST APIs. The rule is COMPLIANT if X-Ray tracing is enabled and NON_COMPLIANT otherwise. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudformation-stack-notification-check | Ensure that your CloudFormation stacks send event notifications to an Amazon SNS topic. Optionally ensure that specified Amazon SNS topics are used. The rule is NON_COMPLIANT if CloudFormation stacks do not send notifications. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | ec2-instance-detailed-monitoring-enabled | Ensure that detailed monitoring is enabled for EC2 instances. The rule is NON_COMPLIANT if detailed monitoring is not enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-action-check | Ensure that CloudWatch alarms have an action configured for the ALARM, INSUFFICIENT_DATA, or OK state. Optionally ensure that any actions match a named ARN. The rule is NON_COMPLIANT if there is no action specified for the alarm or optional parameter. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-resource-check | Ensure that a resource type has a CloudWatch alarm for the named metric. For resource type, you can specify EBS volumes, EC2 instances, Amazon RDS clusters, or S3 buckets. The rule is COMPLIANT if the named metric has a resource ID and CloudWatch alarm. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | cloudwatch-alarm-settings-check | Ensure that CloudWatch alarms with the given metric name have the specified settings. |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | wafv2-rulegroup-logging-enabled | Ensure that Amazon CloudWatch security metrics collection on AWS WAFv2 rule groups is enabled. The rule is NON_COMPLIANT if the 'VisibilityConfig.CloudWatchMetricsEnabled' field is set to false. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| A3.5.1 | Suspicious events are identified and responded to. (PCI-DSS-v4.0) | sns-topic-message-delivery-notification-enabled | Ensure that Amazon Simple Notification Service (SNS) logging is enabled for the delivery status of notification messages sent to a topic for the endpoints. The rule is NON_COMPLIANT if the delivery status notification for messages is not enabled. |

### Template

The template is available on GitHub: Operational Best Practices for PCI DSS 4.0 (Including global resource types).

## Operational Best Practices for Publicly Accessible Resources

This conformance pack helps identify resources that may be publicly accessible.

For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Publicly Accessible Resources.

## Operational Best Practices for RBI Cyber Security Framework for UCBs

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard.

You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Reserve Bank of India (RBI) Cyber Security Framework for Urban Cooperative Banks (UCBs) and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more RBI Cyber Security Framework for UCBs controls. An RBI Cyber Security Framework for UCBs control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.1) | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| Annex_I(1.1) | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant. The lack of centralized account governance may lead to inconsistent account configurations, which |

| Control ID | AWS Config Rule | Guidance |
|---|---|---|
| | | may expose resources and sensitive data. |
| Annex_I(1.1) | ecr-private-tag-immutability-enabled | Enable Elastic Container Repository (ECR) Tag Immutability to prevent image tags on your ECR images from being overwritt en. Previously, tags could be overwritten requiring manual methodologies to uniquely identify an image. |
| Annex_I(1.3) | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired . This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| Annex_I(1.3) | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configure d to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Annex_I(1.3) | api-gw-cache-enabled-and-encrypted | To help protect data at rest, ensure encryption is enabled for your API Gateway stage's cache. Because sensitive data can be captured for the API method, enable encryption at rest to help protect that data. |
| Annex_I(1.3) | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| Annex_I(1.3) | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Annex_I(1.3) | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |
| Annex_I(1.3) | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| Annex_I(1.3) | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | backup-recovery-point-encrypted | Ensure that encryption is enabled for your AWS Backup recovery points. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Annex_I(1.3) | codebuild-project-artifact-encryption | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild artifacts. |
| Annex_I(1.3) | codebuild-project-s3-logs-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your AWS CodeBuild logs stored in Amazon S3. |
| Annex_I(1.3) | opensearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service domains. |
| Annex_I(1.3) | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | opensearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communications within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Annex_I(1.3) | dynamodb-table-encrypted-kms | Ensure that encryption is enabled for your Amazon DynamoDB tables. Because sensitive data can exist at rest in these tables, enable encryption at rest to help protect that data. By default, DynamoDB tables are encrypted with an AWS owned customer master key (CMK). |
| Annex_I(1.3) | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| Annex_I(1.3) | elasticsearch-encrypted-at-rest | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon OpenSearch Service (OpenSearch Service) domains. |
| Annex_I(1.3) | elasticsearch-node-to-node-encryption-check | Ensure node-to-node encryption for Amazon OpenSearch Service is enabled. Node-to-node encryption enables TLS 1.2 encryption for all communica tions within the Amazon Virtual Private Cloud (Amazon VPC). Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryptio n is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| Annex_I(1.3) | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configure d with SSL or HTTPS listeners . Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Annex_I(1.3) | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| Annex_I(1.3) | rds-snapshot-encrypted | Ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) snapshots. Because sensitive data can exist at rest, enable encryption at rest to help protect that data. |
| Annex_I(1.3) | rds-storage-encrypted | To help protect data at rest, ensure that encryption is enabled for your Amazon Relational Database Service (Amazon RDS) instances. Because sensitive data can exist at rest in Amazon RDS instances, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |
| Annex_I(1.3) | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| Annex_I(1.3) | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| Annex_I(1.3) | sagemaker-endpoint-configuration-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker endpoint. Because sensitive data can exist at rest in SageMaker endpoint, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | sagemaker-notebook-instance-kms-key-configured | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your SageMaker notebook. Because sensitive data can exist at rest in SageMaker notebook, enable encryptio n at rest to help protect that data. |
| Annex_I(1.3) | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |
| Annex_I(1.3) | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorable. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| Annex_I(1.3) | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |
| Annex_I(1.3) | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| Annex_I(1.3) | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | autoscaling-launch-config-public-ip-disabled | If you configure your Network Interfaces with a public IP address, then the associated resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessible, as this may allow unintended access to your applications or servers. |
| Annex_I(1.3) | no-unrestricted-route-to-igw | Ensure Amazon EC2 route tables do not have unrestricted routes to an internet gateway. Removing or limiting the access to the internet for workloads within Amazon VPCs can reduce unintended access within your environment. |
| Annex_I(1.3) | redshift-cluster-kms-enabled | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for your Amazon Redshift cluster. Because sensitive data can exist at rest in Redshift clusters, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| Annex_I(1.3) | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |
| Annex_I(1.3) | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| Annex_I(1.3) | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communication between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| Annex_I(1.3) | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |
| Annex_I(1.3) | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organization's policies. |
| Annex_I(1.3) | s3-bucket-level-public-acce ss-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |
| Annex_I(1.3) | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(1.3) | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| Annex_I(1.3) | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventing direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| Annex_I(5.1) | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(5.1) | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| Annex_I(5.1) | waf-regional-rule-not-empty | Ensure your AWS WAF has a rule that is not empty. A rule with no conditions could result in unintended behavior. |
| Annex_I(5.1) | waf-regional-rulegroup-not-empty | Ensure your AWS WAF has a rule group that is not empty. A rule group that is empty could result in unintended behavior. |
| Annex_I(5.1) | waf-regional-webacl-not-empty | A Web ACL attached to an AWS WAF can contain a collection of rules and rule groups to inspect and control web requests. If a Web ACL is empty, the web traffic passes without being detected or acted upon by the WAF. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(5.1) | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |
| Annex_I(5.1) | api-gw-associated-with-waf | AWS WAF enables you to configure a set of rules (called a web access control list (web ACL)) that allow, block, or count web requests based on customizable web security rules and conditions that you define. Ensure your Amazon API Gateway stage is associated with a WAF Web ACL to protect it from malicious attacks |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(5.1) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Annex_I(5.1) | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,3389,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(6) | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |
| Annex_I(6) | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(6) | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |
| Annex_I(6) | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(6) | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relationa l Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |
| Annex_I(6) | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferredMaintenanceWindow (the default is sat:16:00-sat:16:30), and the automatedSnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(6) | vuln-management-plan-exists (process check) | Ensure a vulnerability management plan is developed and implemented in order to have a formally defined processes to address vulnerabilities in your environment. |
| Annex_I(7.1) | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| Annex_I(7.1) | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.1) | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| Annex_I(7.1) | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.1) | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.2) | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| Annex_I(7.3) | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| Annex_I(7.4) | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |
| Annex_I(7.4) | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.4) | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| Annex_I(7.4) | cloudtrail-s3-dataevents-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |
| Annex_I(7.4) | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.4) | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |
| Annex_I(7.4) | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.4) | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |
| Annex_I(7.4) | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed information about your build project. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.4) | opensearch-audit-logging-enabled | Ensure audit logging is enabled on your Amazon OpenSearch Service domains. Audit logging allows you to track user activity on your OpenSearch domains, including authentication successes and failures, requests to OpenSearch, index changes, and incoming search queries. |
| Annex_I(7.4) | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| Annex_I(7.4) | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.4) | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |
| Annex_I(7.4) | rds-logging-enabled | To help with logging and monitoring within your environment, ensure Amazon Relational Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connections, disconnections, queries, or tables queried. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.4) | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |
| Annex_I(7.4) | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(7.4) | wafv2-logging-enabled | To help with logging and monitoring within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, informati on about the request, and an action for the rule that each request matched. |
| Annex_I(7.4) | redshift-cluster-configurat ion-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activitie s in the database. This rule requires that a value is set for clusterDbEncrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(10.2) | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organizat ion from various security breaches or incidents. |
| Annex_I(12) | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |
| Annex_I(12) | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(12) | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |
| Annex_I(12) | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(12) | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Annex_I(12) | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(12) | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(12) | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |
| Annex_I(12) | redshift-backup-enabled | To help with data backup processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(12) | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| Annex_I(12) | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| Annex_I(12) | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

### Template

The template is available on GitHub: Operational Best Practices for RBI Cyber Security Framework for UCBs.

## Operational Best Practices for RBI MD-ITF

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates, are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the Reserve Bank of India (RBI) Master Direction – Information Technology Framework and AWS managed Config rules. Each Config rule applies to a specific AWS resource, and relates to one or more RBI Master Direction – Information Technology Framework controls. An RBI Master Direction – Information Technology Framework control can be related to multiple Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(a) | Identification and Classification of Information Assets. | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 3.1(a) | Identification and Classification of Information Assets. | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | more than the allowed number of days, according to your organization's standards. |
| 3.1(a) | Identification and Classification of Information Assets. | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functionality. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(a) | Identification and Classification of Information Assets. | ecr-private-tag-immutability-enabled | Enable Elastic Container Repository (ECR) Tag Immutability to prevent image tags on your ECR images from being overwritten. Previously, tags could be overwritten requiring manual methodologies to uniquely identify an image. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 3.1(c ) | Role Based Access Control | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |
| 3.1(c ) | Role Based Access Control | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1(c ) | Role Based Access Control | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1(c ) | Role Based Access Control | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1(c ) | Role Based Access Control | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 3.1(c ) | Role Based Access Control | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 3.1(c ) | Role Based Access Control | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 3.1(c ) | Role Based Access Control | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 3.1(c ) | Role Based Access Control | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 3.1(c ) | Role Based Access Control | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(c ) | Role Based Access Control | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(g) | Incident Management | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(g) | Incident Management | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |
| 3.1(g) | Incident Management | alb-waf-enabled | Ensure AWS WAF is enabled on Elastic Load Balancers (ELB) to help protect web applications. A WAF helps to protect your web applications or APIs against common web exploits. These web exploits may affect availability, compromise security, or consume excessive resources within your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(g) | Incident Management | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(g) | Incident Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 3.1(h) | Trails | api-gw-execution-logging-enabled | API Gateway logging displays detailed views of users who accessed the API and the way they accessed the API. This insight enables visibility of user activities. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 3.1(h) | Trails | codebuild-project-logging-enabled | Ensure AWS CodeBuild project logging is enabled so that your build output logs are sent to either Amazon CloudWatch or Amazon Simple Storage Service (Amazon S3). Build output logs provide detailed informati on about your build project. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | opensearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. OpenSearch Service error logs can assist with security and access audits, and can help to diagnose availability issues. |
| 3.1(h) | Trails | redshift-audit-logging-enabled | To capture information about connections and user activities on your Amazon Redshift cluster, ensure audit logging is enabled. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | cloudtrail-enabled | AWS CloudTrail can help in non-repud iation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated , and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |
| 3.1(h) | Trails | cloudtrail-s3-data events-enabled | The collection of Simple Storage Service (Amazon S3) data events helps in detecting any anomalous activity. The details include AWS account information that accessed an Amazon S3 bucket, IP address, and time of event. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | cw-loggroup-retention-period-check | Ensure a minimum duration of event log data is retained for your log groups to help with troubleshooting and forensics investigations. The lack of available past event log data makes it difficult to reconstruct and identify potentially malicious events. |
| 3.1(h) | Trails | elasticsearch-logs-to-cloudwatch | Ensure Amazon OpenSearch Service domains have error logs enabled and streamed to Amazon CloudWatch Logs for retention and response. Domain error logs can assist with security and access audits, and can help to diagnose availability issues. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | elb-logging-enabled | Elastic Load Balancing activity is a central point of communication within an environment. Ensure ELB logging is enabled. The collected data provides detailed information about requests sent to the ELB. Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | multi-region-cloudtrail-enabled | AWS CloudTrail records AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from where the calls were made, and when the calls occurred. CloudTrail will deliver log files from all AWS Regions to your S3 bucket if MULTI_REGION_CLOUD_TRAIL_ENABLED is enabled. Additionally, when AWS launches a new Region, CloudTrail will create the same trail in the new Region. As a result, you will receive log files containing API activity for the new Region without taking any action. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | rds-logging-enabled | To help with logging and monitorin g within your environment, ensure Amazon Relationa l Database Service (Amazon RDS) logging is enabled. With Amazon RDS logging, you can capture events such as connectio ns, disconnections, queries, or tables queried. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for information about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | wafv2-logging-enabled | To help with logging and monitorin g within your environment, enable AWS WAF (V2) logging on regional and global web ACLs. AWS WAF logging provides detailed information about the traffic that is analyzed by your web ACL. The logs record the time that AWS WAF received the request from your AWS resource, information about the request, and an action for the rule that each request matched. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(h) | Trails | redshift-cluster-configuration-check | To protect data at rest, ensure that encryption is enabled for your Amazon Redshift clusters. You must also ensure that required configurations are deployed on Amazon Redshift clusters. The audit logging should be enabled to provide information about connections and user activities in the database. This rule requires that a value is set for clusterDb Encrypted (Config Default : TRUE), and loggingEnabled (Config Default: TRUE). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(i) | Public Key Infrastructure | acm-certificate-expiration-check | Ensure network integrity is protected by ensuring X509 certificates are issued by AWS ACM. These certificates must be valid and unexpired. This rule requires a value for daysToExpiration (AWS Foundational Security Best Practices value: 90). The actual value should reflect your organization's policies. |
| 3.1(i) | Public Key Infrastructure | alb-http-drop-invalid-header-enabled | Ensure that your Elastic Load Balancers (ELB) are configured to drop http headers. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(i) | Public Key Infrastructure | alb-http-to-https-redirection-check | To help protect data in transit, ensure that your Application Load Balancer automatically redirects unencrypted HTTP requests to HTTPS. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1(i) | Public Key Infrastructure | api-gw-ssl-enabled | Ensure Amazon API Gateway REST API stages are configured with SSL certificates to allow backend systems to authenticate that requests originate from API Gateway. |
| 3.1(i) | Public Key Infrastructure | opensearch-https-required | Because sensitive data can exist and to help protect data in transit, ensure HTTPS is enabled for connections to your Amazon OpenSearch Service domains. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(i) | Public Key Infrastructure | elbv2-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |
| 3.1(i) | Public Key Infrastructure | elb-acm-certificate-required | Because sensitive data can exist and to help protect data at transit, ensure encryption is enabled for your Elastic Load Balancing. Use AWS Certificate Manager to manage, provision and deploy public and private SSL/TLS certificates with AWS services and internal resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(i) | Public Key Infrastructure | elb-tls-https-listeners-only | Ensure that your Elastic Load Balancers (ELBs) are configured with SSL or HTTPS listeners. Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.1(i) | Public Key Infrastructure | redshift-require-tls-ssl | Ensure that your Amazon Redshift clusters require TLS/SSL encryption to connect to SQL clients. Because sensitive data can exist, enable encryption in transit to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.1(i) | Public Key Infrastructure | s3-bucket-ssl-requests-only | To help protect data in transit, ensure that your Amazon Simple Storage Service (Amazon S3) buckets require requests to use Secure Socket Layer (SSL). Because sensitive data can exist, enable encryption in transit to help protect that data. |
| 3.3 | Vulnerability Management | elastic-beanstalk-managed-updates-enabled | Enabling managed platform updates for an Amazon Elastic Beanstalk environment ensures that the latest available platform fixes, updates, and features for the environment are installed. Keeping up to date with patch installation is a best practice in securing systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Vulnerability Management | rds-automatic-minor-version-upgrade-enabled | Enable automatic minor version upgrades on your Amazon Relational Database Service (RDS) instances to ensure the latest minor version updates to the Relational Database Management System (RDBMS) are installed, which may include security patches and bug fixes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Vulnerability Management | redshift-cluster-maintenancesettings-check | This rule ensures that Amazon Redshift clusters have the preferred settings for your organization. Specifically, that they have preferred maintenance windows and automated snapshot retention periods for the database. This rule requires you to set the allowVersionUpgrade. The default is true. It also lets you optionally set the preferred MaintenanceWindow (the default is sat:16:00-sat:16:30), and the automated SnapshotRetentionPeriod (the default is 1). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Vulnerability Management | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Vulnerability Management | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Vulnerability Management | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.3 | Vulnerability Management | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5 | Cyber Crisis Management Plan | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5 | Cyber Crisis Management Plan | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5 | Cyber Crisis Management Plan | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5 | Cyber Crisis Management Plan | ec2-managedinstance-association-compliance-status-check | Use AWS Systems Manager Associations to help with inventory of software platforms and applications within an organization. AWS Systems Manager assigns a configuration state to your managed instances and allows you to set baselines of operating system patch levels, software installations, application configurations, and other details about your environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.5 | Cyber Crisis Management Plan | ec2-managedinstance-patch-compliance-status-check | Enable this rule to help with identification and documentation of Amazon Elastic Compute Cloud (Amazon EC2) vulnerabilities. The rule checks if Amazon EC2 instance patch compliance in AWS Systems Manager as required by your organization's policies and procedures. |
| 3.9 | IT Risk Assessment | annual-risk-assessment-performed (process check) | Perform an annual risk assessment on your organization. Risk assessments can assist in determining the likelihood and impact of identified risks and/or vulnerabilities affecting an organization. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 3.12 | Training | security-awareness-program-exists (process check) | Establish and maintain a security awareness program for your organization. Security awareness programs educate employees on how to protect their organization from various security breaches or incidents. |
| 4.4(g) | Fraud analysis-Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, manipulation of financial records etc. The regulatory requirement of reporting fraud to RBI should be system driven. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 4.4(h) | Capacity and performance analysis of IT security systems. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | clb-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |
| 4.4(h) | Capacity and performance analysis of IT security systems. | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | lambda-vpc-multi-az-check | If your AWS Lambda function is configure d to connect to a virtual private cloud (VPC) in your account, deploy the AWS Lambda function in at least two different Availability Zones to ensure that it is your function is available to process events in case of a service interruption in a single zone. |
| 4.4(h) | Capacity and performance analysis of IT security systems. | rds-instance-delet ion-protection-ena bled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | s3-bucket-default-lock-enabled | Ensure that your Amazon Simple Storage Service (Amazon S3) bucket has lock enabled, by default. Because sensitive data can exist at rest in S3 buckets, enforce object locks at rest to help protect that data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| 4.4(h) | Capacity and performance analysis of IT security systems. | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |
| 4.4(h) | Capacity and performance analysis of IT security systems. | lambda-dlq-check | Enable this rule to help notify the appropriate personnel through Amazon Simple Queue Service (Amazon SQS) or Amazon Simple Notification Service (Amazon SNS) when a function has failed. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | beanstalk-enhanced-health-reporting-enabled | AWS Elastic Beanstalk enhanced health reporting enables a more rapid response to changes in the health of the underlying infrastructure. These changes could result in a lack of availability of the application. Elastic Beanstalk enhanced health reporting provides a status descriptor to gauge the severity of the identified issues and identify possible causes to investigate. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connectio ns, devices, and software. AWS Security Hub aggregates, organizes , and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(h) | Capacity and performance analysis of IT security systems. | ebs-optimized-instance | An optimized instance in Amazon Elastic Block Store (Amazon EBS) provides additional, dedicated capacity for Amazon EBS I/O operations. This optimization provides the most efficient performance for your EBS volumes by minimizing contention between Amazon EBS I/O operations and other traffic from your instance. |
| 4.4(h) | Capacity and performance analysis of IT security systems. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(i) | Incident reporting , their impact and steps taken for non -recurrence of such events in the future. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpecte d, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 4.4(i) | Incident reporting, their impact and steps taken for non-recurrence of such events in the future. | guardduty-non-archived-findings | Amazon GuardDuty helps you understand the impact of an incident by classifying findings by severity: low, medium, and high. You can use these classifications for determining remediation strategies and priorities. This rule allows you to optionally set the daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7), and daysHighSev (Config Default: 1) for non-archived findings, as required by your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | aurora-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Aurora resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | cmk-backing-key-rotation-enabled | Enable key rotation to ensure that keys are rotated after they have reached the end of their crypto period. |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | ec2-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Compute Cloud (Amazon EC2) resources are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | fsx-resources-protected-by-backup-plan | To help with data back-up processes, ensure your Amazon FSx file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 6.3 | NBFCs shall consider the need to put in place necessary backup sites for their critical business systems and Data centers. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | dynamodb-autoscaling-enabled | Amazon DynamoDB auto scaling uses the AWS Application Auto Scaling service to adjust provisioned throughput capacity that automatically responds to actual traffic patterns. This enables a table or a global secondary index to increase its provisioned read/write capacity to handle sudden increases in traffic, without throttling. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | elb-cross-zone-load-balancing-enabled | Enable cross-zone load balancing for your Elastic Load Balancers (ELBs) to help maintain adequate capacity and availability. The cross-zone load balancing reduces the need to maintain equivalent numbers of instances in each enabled availability zone. It also improves your application's ability to handle the loss of one or more instances. |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | elb-deletion-protection-enabled | This rule ensures that Elastic Load Balancing has deletion protection enabled. Use this feature to prevent your load balancer from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | clb-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | elbv2-multiple-az | Elastic Load Balancing (ELB) automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in an availability zone. To ensure high availability, ensure your ELB has registered instances from multiple Availability Zones. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | lambda-vpc-multi-az-check | If your AWS Lambda function is configure d to connect to a virtual private cloud (VPC) in your account, deploy the AWS Lambda function in at least two different Availability Zones to ensure that it is your function is available to process events in case of a service interruption in a single zone. |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | rds-instance-deletion-protection-enabled | Ensure Amazon Relational Database Service (Amazon RDS) instances have deletion protectio n enabled. Use deletion protection to prevent your Amazon RDS instances from being accidentally or maliciously deleted, which can lead to loss of availability for your applications. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | rds-multi-az-support | Multi-AZ support in Amazon Relationa l Database Service (Amazon RDS) provides enhanced availability and durability for database instances. When you provision a Multi-AZ database instance, Amazon RDS automatically creates a primary database instance, and synchronously replicates the data to a standby instance in a different Availabil ity Zone. Each Availability Zone runs on its own physicall y distinct, independe nt infrastructure, and is engineered to be highly reliable. In case of an infrastru cture failure, Amazon RDS performs an automatic failover to the standby so that you can resume database operation s as soon as the failover is complete. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | vpc-vpn-2-tunnels-up | Redundant Site-to-Site VPN tunnels can be implemented to achieve resilience requirements. It uses two tunnels to help ensure connectivity in case one of the Site-to-Site VPN connections becomes unavailable. To protect against a loss of connectivity, in case your customer gateway becomes unavailable, you can set up a second Site-to-Site VPN connection to your Amazon Virtual Private Cloud (Amazon VPC) and virtual private gateway by using a second customer gateway. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | autoscaling-group-elb-healthcheck-required | The Elastic Load Balancer (ELB) health checks for Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling groups support maintenance of adequate capacity and availability. The load balancer periodically sends pings, attempts connections, or sends requests to test Amazon EC2 instances health in an auto-scaling group. If an instance is not reporting back, traffic is sent to a new Amazon EC2 instance. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | dynamodb-throughput-limit-check | Enable this rule to ensure that provisioned throughput capacity is checked on your Amazon DynamoDB tables. This is the amount of read/write activity that each table can support. DynamoDB uses this information to reserve sufficient system resources to meet your throughput requirements. This rule generates an alert when the throughput approaches the maximum limit for a customer's account. This rule allows you to optionally set accountRCUThresholdPercentage (Config Default: 80) and accountWCUThresholdPercentage (Config Default: 80) parameters. The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | guardduty-enabled-centralized | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intelligence feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | lambda-concurrency-check | This rule ensures that a Lambda function's concurrency high and low limits are established. This can assist in baselining the number of requests that your function is serving at any given time. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | rds-enhanced-monitoring-enabled | Enable Amazon Relational Database Service (Amazon RDS) to help monitor Amazon RDS availability. This provides detailed visibility into the health of your Amazon RDS database instances. When the Amazon RDS storage is using more than one underlying physical device, Enhanced Monitoring collects the data for each device. Also, when the Amazon RDS database instance is running in a Multi-AZ deployment, the data for each device on the secondary host is collected, and the secondary host metrics. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.1 | IT Systems should be progressively scaled up as the size and complexity of NBFC's operations increases. | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | dms-replication-not-public | Manage access to the AWS Cloud by ensuring DMS replication instances cannot be publicly accessed. DMS replication instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | ebs-snapshot-public-restorable-check | Manage access to the AWS Cloud by ensuring EBS snapshots are not publicly restorabl e. EBS volume snapshots can contain sensitive information and access control is required for such accounts. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | elasticsearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service (OpenSearch Service) Domains are within an Amazon Virtual Private Cloud (Amazon VPC). An OpenSearch Service domain within an Amazon VPC enables secure communication between OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | emr-master-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon EMR cluster master nodes cannot be publicly accessed. Amazon EMR cluster master nodes can contain sensitive information and access control is required for such accounts. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communica tion between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints . Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorized Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthorized access to Amazon VPC resources. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requireme nt for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | rds-instance-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information, and principles and access control is required for such accounts. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | rds-snapshots-public-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Relational Database Service (Amazon RDS) instances are not public. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | redshift-cluster-public-access-check | Manage access to resources in the AWS Cloud by ensuring that Amazon Redshift clusters are not public. Amazon Redshift clusters can contain sensitive information and principles and access control is required for such accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confident iality of systems. This rule allows you to optionall y set blockedPo rt1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | sagemaker-notebook-no-direct-internet-access | Manage access to resources in the AWS Cloud by ensuring that Amazon SageMaker notebooks do not allow direct internet access. By preventin g direct internet access, you can keep sensitive data from being accessed by unauthorized users. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricti ng all the traffic on the default security group helps in restricting remote access to your AWS resources. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | access-keys-rotated | The credentials are audited for authorize d devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromis ed. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | emr-kerberos-enabled | The access permissions and authorizations can be managed and incorporated with the principles of least privilege and separation of duties, by enabling Kerberos for Amazon EMR clusters. In Kerberos, the services and the users that need to authenticate are known as principals. The principals exist within a Kerberos realm. Within the realm, a Kerberos server is known as the key distribution center (KDC). It provides a means for the principals to authenticate. The KDC authenticates by issuing tickets for authentication. The KDC maintains a database of the principals within its realm, their passwords, and other administrative |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | information about each principal. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-group-has-users-check | AWS Identity and Access Managemen t (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissio ns and authoriza tions, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissio ns or job function is one way to incorpora te least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | autoscaling-launch -config-public-ip- disabled | If you configure your Network Interfaces with a public IP address, then the associate d resources to those Network Interfaces are reachable from the internet. EC2 resources should not be publicly accessibl e, as this may allow unintended access to your applications or servers. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-policy-no-statements-with-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | ecs-task-definition-nonroot-user | To assist with implementing the principle of least privilege, ensure that a non-root user is designated for access to your Amazon Elastic Container Service (Amazon ECS) task definitions. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | efs-access-point-enforce-root-directory | Enforcing a root directory for an Amazon Elastic File System (Amazon EFS) access point helps restrict data access by ensuring that users of the access point can only reach files of the specified subdirectory. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | efs-access-point-enforce-user-identity | To assist with implementing the principle of least privilege, ensure user enforcement is enabled for your Amazon Elastic File System (Amazon EFS) .When enabled, Amazon EFS replaces the NFS client's user and group IDs with the identity configured on the access point for all file system operations and only grants access to this enforced user identity. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | subnet-auto-assign-public-ip-disabled | Manage access to the AWS Cloud by ensuring Amazon Virtual Private Cloud (VPC) subnets are not automatically assigned a public IP address. Amazon Elastic Compute Cloud (EC2) instances that are launched into subnets that have this attribute enabled have a public IP address assigned to their primary network interface. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Managemen t (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-based AWS accounts to help to incorporate the principle of least functionality. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-user-group-membership-check | AWS Identity and Access Managemen t (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privilege s than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | opensearch-in-vpc-only | Manage access to the AWS Cloud by ensuring Amazon OpenSearch Service domains are within an Amazon Virtual Private Cloud (Amazon VPC). An Amazon OpenSearch Service domain within an Amazon VPC enables secure communication between Amazon OpenSearch Service and other services within the Amazon VPC without the need for an internet gateway, NAT device, or VPN connection. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protection for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.I | Basic security aspects such as physical/ logical access controls and well defined password policy. | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| 8.II | A well-defined user role. | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.II | A well-defined user role. | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissio ns management. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.II | A well-defined user role. | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizat ional IAM password policy. They meet or exceed requireme nts as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUppercaseCh aracters (AWS Foundational Security Best Practices value: true), RequireLo wercaseCharacters (AWS Foundatio nal Security Best Practices value: true), RequireSymbols (AWS Foundatio nal Security Best Practices value: true), RequireNumbers (AWS Foundatio nal Security Best Practices value: true), MinimumPa |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| | | | sswordLength (AWS Foundational Security Best Practices value: 14), PasswordR eusePrevention (AWS Foundatio nal Security Best Practices value: 24), and MaxPasswordAge (AWS Foundatio nal Security Best Practices value: 90) for your IAM Password Policy. The actual values should reflect your organizat ion's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.II | A well-defined user role. | iam-policy-no-statements-with-admin-access | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricting policies from containing "Effect": "Allow" with "Action": "*" over "Resource": "*". Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.II | A well-defined user role. | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authorizations, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |
| 8.II | A well-defined user role. | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.II | A well-defined user role. | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissions and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsageAge (Config Default: 90). The actual value should reflect your organization's policies. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.III | A Maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/ information. | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and applicati on failures. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | db-instance-backup-enabled | The backup feature of Amazon RDS creates backups of your databases and transaction logs. Amazon RDS automatically creates a storage volume snapshot of your DB instance, backing up the entire DB instance. The system allows you to set specific retention periods to meet your resilience requireme nts. |

| Control ID | Control Description | AWS Config Rule | Guidance |
|---|---|---|---|
| 8.IX | Arrangement for backup of data with periodic testing. | dynamodb-in-backup-plan | To help with data back-up processes, ensure your Amazon DynamoDB tables are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |
| 8.IX | Arrangement for backup of data with periodic testing. | dynamodb-pitr-enabled | Enable this rule to check that information has been backed up. It also maintains the backups by ensuring that point-in-time recovery is enabled in Amazon DynamoDB. The recovery maintains continuous backups of your table for the last 35 days. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | elasticache-redis-cluster-automatic-backup-check | When automatic backups are enabled, Amazon ElastiCache creates a backup of the cluster on a daily basis. The backup can be retained for a number of days as specified by your organization. Automatic backups can help guard against data loss. If a failure occurs, you can create a new cluster, which restores your data from the most recent backup. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | rds-in-backup-plan | To help with data back-up processes, ensure your Amazon Relational Database Service (Amazon RDS) instances are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifie s your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | s3-bucket-replication-enabled | Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) supports maintaining adequate capacity and availability. CRR enables automatic, asynchronous copying of objects across Amazon S3 buckets to help ensure that data availability is maintained. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | redshift-backup-enabled | To help with data back-up processes, ensure your Amazon Redshift clusters have automated snapshots. When automated snapshots are enabled for a cluster, Redshift periodically takes snapshots of that cluster. By default, Redshift takes a snapshot every eight hours or every 5 GB for each node of data changes, or whichever comes first. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | backup-plan-min-frequency-and-min-retention-check | To help with data back-up processes, ensure your AWS Backup plan is set for a minimum frequency and retention. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) and requiredFrequencyUnit (Config default: days) parameters. The actual value should reflect your organizations requirements. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | backup-recovery-point-manual-deletion-disabled | Ensure that your AWS Backup recovery points have an attached resource-based policy which prevents deletion of recovery points. Using a resource-based policy to prevent deletion of recovery points can assist in preventin g accidental or intentional deletion. |

| Control ID | Control Description | AWS Config Rule | Guidance |
| --- | --- | --- | --- |
| 8.IX | Arrangement for backup of data with periodic testing. | backup-recovery-point-minimum-retention-check | To help with data back-up processes, ensure your AWS Backup recovery points have a minimum retention period set. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. This rule allows you to set the requiredRetentionDays (config default: 35) parameter. The actual value should reflect your organizations requirements. |

## Template

The template is available on GitHub: Operational Best Practices for RBI MD-ITF.

## Operational Best Practices for Security, Identity, and Compliance Services

This conformance pack contains AWS Config rules based on Security, Identity, and Compliance Services. For more information, see Security, Identity, and Compliance on AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Security, Identity, and Compliance Services.

## Operational Best Practices for Serverless

This conformance pack contains AWS Config rules based on Serverless solutions. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Serverless.

## Operational Best Practices for Storage Services

This conformance pack contains AWS Config rules based on Storage Services. For more information, see Cloud Storage on AWS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Operational Best Practices for Storage Services.

## Operational Best Practices for SWIFT CSP

Conformance packs provide a general-purpose compliance framework designed to enable you to create security, operational or cost-optimization governance checks using managed or custom AWS Config rules and AWS Config remediation actions. Conformance Packs, as sample templates,

are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

The following provides a sample mapping between the SWIFT's Customer Security Programme (CSP) and AWS managed Config rules. Each AWS Config rule applies to a specific AWS resource, and relates to one or more SWIFT CSP controls. A SWIFT CSP control can be related to multiple AWS Config rules. Refer to the table below for more detail and guidance related to these mappings.

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.1 | ec2-instance-managed-by-systems-manager | An inventory of the software platforms and applications within the organization is possible by managing Amazon Elastic Compute Cloud (Amazon EC2) instances with AWS Systems Manager. Use AWS Systems Manager to provide detailed system configurations, operating system patch levels, services name and type, software installations, application name, publisher and version, and other details about your environment. |
| 1.1 | ec2-instance-no-public-ip | Manage access to the AWS Cloud by ensuring Amazon Elastic Compute Cloud (Amazon EC2) instances cannot be publicly accessed. Amazon EC2 instances can contain sensitive information and access control is required for such accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.1 | ec2-no-amazon-key-pair | This rule checks if running Amazon Elastic Compute Cloud (Amazon EC2) instances are launched using amazon key pairs. This can assist in reducing the risk of compromised credentia ls. Amazon EC2 Instances without key pairs can still be accessed using Session Manager or Browser based SSH connection from the AWS console. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.1 | ec2-instances-in-vpc | Deploy Amazon Elastic Compute Cloud (Amazon EC2) instances within an Amazon Virtual Private Cloud (Amazon VPC) to enable secure communication between an instance and other services within the amazon VPC, without requiring an internet gateway, NAT device, or VPN connection. All traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. Assign Amazon EC2 instances to an Amazon VPC to properly manage access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.1 | vpc-default-security-group-closed | Amazon Elastic Compute Cloud (Amazon EC2) security groups can help in the management of network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Restricting all the traffic on the default security group helps in restricting remote access to your AWS resources. |
| 1.1 | vpc-network-acl-unused-check | This rule ensures that Amazon Virtual Private Cloud (VPC) network access control lists are in use. Monitoring for unused network access control lists can assist in accurate inventory and management of your environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.1 | vpc-sg-open-only-to-authorized-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) Security Groups. Not restricting access on ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. By restricting access to resources within a security group from the internet (0.0.0.0/0) remote access can be controlled to internal systems. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | iam-customer-policy-blocked-kms-actions | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, restricti ng policies from containin g blocked actions on all AWS Key Management Service keys. Having more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. This rule allows you to set the blockedActionsPatt erns parameter. (AWS Foundational Security Best Practices value: kms:Decry pt, kms:ReEncryptFrom). The actual values should reflect your organization's policies |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | iam-group-has-users-check | AWS Identity and Access Management (IAM) can help you incorporate the principles of least privilege and separation of duties with access permissions and authorizations, by ensuring that IAM groups have at least one user. Placing users in groups based on their associated permissions or job function is one way to incorporate least privilege. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | iam-inline-policy-blocked-kms-actions | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to allow blocked actions on all AWS Key Management Service keys. AWS recommends to use managed policies instead of inline policies. The managed policies allow reusability, versioning, rolling back, and delegating permissions management. This rule allows you to set the blockedActionsPatterns parameter. (AWS Foundational Security Best Practices value: kms:Decrypt, kms:ReEncryptFrom). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | iam-no-inline-policy-check | Ensure an AWS Identity and Access Management (IAM) user, IAM role or IAM group does not have an inline policy to control access to systems and assets. AWS recommend s to use managed policies instead of inline policies. The managed policies allow reusability, versioning and rolling back, and delegating permissions management. |
| 1.2 | iam-user-no-policies-check | This rule ensures AWS Identity and Access Management (IAM) policies are attached only to groups or roles to control access to systems and assets. Assigning privileges at the group or the role level helps to reduce opportunity for an identity to receive or retain excessive privileges. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | restricted-ssh | Amazon Elastic Compute Cloud (Amazon EC2) Security Groups can help manage network access by providing stateful filtering of ingress and egress network traffic to AWS resources. Not allowing ingress (or remote) traffic from 0.0.0.0/0 to port 22 on your resources help you restricting remote access. |
| 1.2 | nacl-no-unrestricted-ssh-rdp | Access to remote server administration ports in your Network Access Control Lists (NACLs), such as port 22 (SSH) and port 3389 (RDP), should not be publicly accessible, as this may allow unintende d access to resources within your VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | s3-bucket-acl-prohibited | This rule checks to see if Access Control Lists (ACLs) are used to for access control on Amazon S3 Buckets. ACLs are legacy access control mechanisms for Amazon S3 buckets that predate AWS Identity and Access Management (IAM). Instead of ACLs, it is a best practice to use IAM policies or S3 bucket policies to more easily manage access to your S3 buckets. |
| 1.2 | s3-bucket-logging-enabled | Amazon Simple Storage Service (Amazon S3) server access logging provides a method to monitor the network for potential cybersecurity events. The events are monitored by capturing detailed records for the requests that are made to an Amazon S3 bucket. Each access log record provides details about a single access request. The details include the requester, bucket name, request time, request action, response status, and an error code, if relevant. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | s3-bucket-policy-grantee-check | Manage access to the AWS Cloud by enabling s3_ bucket_policy_grantee_check. This rule checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or Amazon Virtual Private Cloud (Amazon VPC) IDs that you provide. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.2 | sns-topic-message-delivery-notification-enabled | To assist with logging requirements in your environment, ensure to enable delivery status notifications are enabled for your Amazon Simple Notification Service (Amazon SNS) topics. Logging message delivery status helps provide better operational insight, such as the following: Knowing whether a message was delivered to the Amazon SNS endpoint, identifying the response sent from the Amazon SNS endpoint to Amazon SNS, and determining the message dwell time (the time between the publish timestamp and just before handing off to an Amazon SNS endpoint). |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.4 | internet-gateway-authorized-vpc-only | Manage access to resources in the AWS Cloud by ensuring that internet gateways are only attached to authorize d Amazon Virtual Private Cloud (Amazon VPC). Internet gateways allow bi-directional internet access to and from the Amazon VPC that can potentially lead to unauthori zed access to Amazon VPC resources. |
| 1.4 | restricted-common-ports | Manage access to resources in the AWS Cloud by ensuring common ports are restricted on Amazon Elastic Compute Cloud (Amazon EC2) security groups. Not restricting access to ports to trusted sources can lead to attacks against the availability, integrity and confidentiality of systems. This rule allows you to optionally set blockedPort1 - blockedPort5 parameters (Config Defaults: 20,21,338 9,3306,4333). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.4 | lambda-function-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring AWS Lambda functions cannot be publicly accessed. Public access can potentially lead to degradation of availability of resources. |
| 1.4 | s3-account-level-public-access-blocks-periodic | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access. This rule allows you to optionally set the ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True), and restrictPublicBuckets parameters (Config Default: True). The actual values should reflect your organization's policies. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.4 | s3-bucket-level-public-access-prohibited | Manage access to resources in the AWS Cloud by ensuring that Amazon Simple Storage Service (Amazon S3) buckets cannot be publicly accessed. This rule helps keeping sensitive data safe from unauthorized remote users by preventing public access at the bucket level. |
| 1.4 | s3-bucket-public-read-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |
| 1.4 | s3-bucket-public-write-prohibited | Manage access to resources in the AWS Cloud by only allowing authorized users, processes, and devices access to Amazon Simple Storage Service (Amazon S3) buckets. The management of access should be consistent with the classification of the data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 1.4 | ssm-document-not-public | Ensure AWS Systems Manager (SSM) documents are not public, as this may allow unintended access to your SSM documents. A public SSM document can expose information about your account, resources and internal processes. |
| 2.3 | ec2-imdsv2-check | Ensure the Instance Metadata Service Version 2 (IMDSv2) method is enabled to help protect access and control of Amazon Elastic Compute Cloud (Amazon EC2) instance metadata. The IMDSv2 method uses session-b ased controls. With IMDSv2, controls can be implemented to restrict changes to instance metadata. |
| 2.3 | ec2-instance-multiple-eni-c heck | This rule checks if your Amazon Elastic Compute Cloud (Amazon EC2) instances have multiple ENIs. Having multiple ENIs can cause dual-homed instances, meaning instances that have multiple subnets. This can add network security complexity and introduce unintended network paths and access. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.3 | ec2-token-hop-limit-check | Ensure the Instance Metadata Service (IMDS) HTTP PUT response is restricted to the Amazon Elastic Compute Cloud (Amazon EC2) instance. With IMDSv2, the PUT response that contains the secret token by default cannot travel outside the instance, because the Metadata response hop limit is set to 1 (Config default). If this value is greater than 1, the token is able to leave the EC2 instance. |
| 2.3 | ec2-volume-inuse-check | This rule ensures that Amazon Elastic Block Store volumes that are attached to Amazon Elastic Compute Cloud (Amazon EC2) instances are marked for deletion when an instance is terminated. If an Amazon EBS volume isn't deleted when the instance that it's attached to is terminated, it may violate the concept of least functiona lity. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.3 | account-part-of-organizations | Centralized management of AWS accounts within AWS Organizations helps to ensure that accounts are compliant . The lack of centralized account governance may lead to inconsistent account configurations, which may expose resources and sensitive data. |
| 2.3 | lambda-inside-vpc | Deploy AWS Lambda functions within an Amazon Virtual Private Cloud (Amazon VPC) for a secure communica tion between a function and other services within the Amazon VPC. With this configuration, there is no requirement for an internet gateway, NAT device, or VPN connection. All the traffic remains securely within the AWS Cloud. Because of their logical isolation, domains that reside within an Amazon VPC have an extra layer of security when compared to domains that use public endpoints. To properly manage access, AWS Lambda functions should be assigned to a VPC. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.3 | kms-cmk-not-scheduled-for-deletion | To help protect data at rest, ensure necessary customer master keys (CMKs) are not scheduled for deletion in AWS Key Management Service (AWS KMS). Because key deletion is necessary at times, this rule can assist in checking for all keys scheduled for deletion, in case a key was scheduled unintentionally. |
| 2.3 | s3-bucket-versioning-enabled | Amazon Simple Storage Service (Amazon S3) bucket versioning helps keep multiple variants of an object in the same Amazon S3 bucket. Use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. Versioning helps you to easily recover from unintended user actions and application failures. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.3 | secretsmanager-secret-unused | If unused credentials exist in AWS Secrets Manager, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule allows you to set a value to the unusedForDays (Config Default: 90). The actual value should reflect your organization's policies. |
| 2.5A | ebs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic Block Store (Amazon EBS) volumes are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5A | ec2-ebs-encryption-by-default | To help protect data at rest, ensure that encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. Because sensitive data can exist at rest in these volumes, enable encryption at rest to help protect that data. |
| 2.5A | efs-encrypted-check | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic File System (EFS). |
| 2.5A | efs-in-backup-plan | To help with data back-up processes, ensure your Amazon Elastic File System (Amazon EFS) file systems are a part of an AWS Backup plan. AWS Backup is a fully managed backup service with a policy-based backup solution. This solution simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5A | encrypted-volumes | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Elastic Block Store (Amazon EBS) volumes. |
| 2.5A | kinesis-stream-encrypted | Because sensitive data can exist and to help protect data at rest, ensure encryption is enabled for your Amazon Kinesis Streams. |
| 2.5A | s3-bucket-server-side-encryption-enabled | To help protect data at rest, ensure encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in Amazon S3 buckets, enable encryption to help protect that data. |
| 2.5A | s3-default-encryption-kms | Ensure that encryption is enabled for your Amazon Simple Storage Service (Amazon S3) buckets. Because sensitive data can exist at rest in an Amazon S3 bucket, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 2.5A | sns-encrypted-kms | To help protect data at rest, ensure that your Amazon Simple Notification Service (Amazon SNS) topics require encryption using AWS Key Management Service (AWS KMS). Because sensitive data can exist at rest in published messages, enable encryptio n at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.1 | iam-password-policy | The identities and the credentials are issued, managed, and verified based on an organizational IAM password policy. They meet or exceed requirements as stated by NIST SP 800-63 and the AWS Foundatio nal Security Best Practices standard for password strength. This rule allows you to optionally set RequireUp percaseCharacters (AWS Foundational Security Best Practices value: true), RequireLowercaseCharacters (AWS Foundational Security Best Practices value: true), RequireSymbols (AWS Foundational Security Best Practices value: true), RequireNumbers (AWS Foundational Security Best Practices value: true), MinimumPasswordLength (AWS Foundational Security Best Practices value: 14), PasswordReusePrevention (AWS Foundational Security Best Practices value: 24), and MaxPasswordAge (AWS Foundational Security Best Practices value: 90) for your IAM Password Policy. The |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| | | actual values should reflect your organization's policies. |
| 4.1 | access-keys-rotated | The credentials are audited for authorized devices, users, and processes by ensuring IAM access keys are rotated as specified by the organizational policy. Changing the access keys on a regular schedule is a security best practice. It shortens the period an access key is active and reduces the business impact if the keys are compromised. This rule requires an access key rotation value (Config Default: 90). The actual value should reflect your organizat ion's policies. |
| 4.2 | iam-user-mfa-enabled | Enable this rule to restrict access to resources in the AWS Cloud. This rule ensures multi-factor authentication (MFA) is enabled for all users. MFA adds an extra layer of protection on top of sign-in credentials. Reduce the incidents of compromised accounts by requiring MFA for users. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.2 | mfa-enabled-for-iam-console-access | Manage access to resources in the AWS Cloud by ensuring that MFA is enabled for all AWS Identity and Access Management (IAM) users that have a console password. MFA adds an extra layer of protection on top of sign-in credentials. By requiring MFA for users, you can reduce incidents of compromised accounts and keep sensitive data from being accessed by unauthorized users. |
| 4.2 | root-account-hardware-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring hardware MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 4.2 | root-account-mfa-enabled | Manage access to resources in the AWS Cloud by ensuring MFA is enabled for the root user. The root user is the most privileged user in an AWS account. The MFA adds an extra layer of protectio n for sign-in credentials. By requiring MFA for the root user, you can reduce the incidents of compromised AWS accounts. |
| 5.1 | ec2-instance-profile-attached | EC2 instance profiles pass an IAM role to an EC2 instance. Attaching an instance profile to your instances can assist with least privilege and permissions management. |
| 5.1 | iam-policy-no-statements-wi th-full-access | Ensure IAM Actions are restricted to only those actions that are needed. Allowing users to have more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 5.1 | iam-root-access-key-check | Access to systems and assets can be controlled by checking that the root user does not have access keys attached to their AWS Identity and Access Management (IAM) role. Ensure that the root access keys are deleted. Instead, create and use role-base d AWS accounts to help to incorporate the principle of least functionality. |
| 5.1 | iam-user-group-membership-check | AWS Identity and Access Management (IAM) can help you restrict access permissions and authoriza tions, by ensuring users are members of at least one group. Allowing users more privileges than needed to complete a task may violate the principle of least privilege and separation of duties. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 5.1 | iam-user-unused-credentials-check | AWS Identity and Access Management (IAM) can help you with access permissio ns and authorizations by checking for IAM passwords and access keys that are not used for a specified time period. If these unused credentials are identified, you should disable and/or remove the credentials, as this may violate the principle of least privilege. This rule requires you to set a value to the maxCredentialUsage Age (Config Default: 90). The actual value should reflect your organization's policies. |
| 5.4 | secretsmanager-rotation-enabled-check | This rule ensures AWS Secrets Manager secrets have rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 5.4 | secretsmanager-scheduled-rotation-success-check | This rule ensures that AWS Secrets Manager secrets have rotated successfully according to the rotation schedule. Rotating secrets on a regular schedule can shorten the period that a secret is active, and potentially reduce the business impact if it is compromised. |
| 5.4 | secretsmanager-secret-periodic-rotation | This rule ensures AWS Secrets Manager secrets have periodic rotation enabled. Rotating secrets on a regular schedule can shorten the period a secret is active, and potentially reduce the business impact if the secret is compromised. The default value is 90 days. |
| 5.4 | secretsmanager-using-cmk | To help protect data at rest, ensure encryption with AWS Key Management Service (AWS KMS) is enabled for AWS Secrets Manager secrets. Because sensitive data can exist at rest in Secrets Manager secrets, enable encryption at rest to help protect that data. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4 | ec2-instance-detailed-monitoring-enabled | Enable this rule to help improve Amazon Elastic Compute Cloud (Amazon EC2) instance monitoring on the Amazon EC2 console, which displays monitoring graphs with a 1-minute period for the instance. |
| 6.4 | cloudwatch-log-group-encrypted | To help protect sensitive data at rest, ensure encryption is enabled for your Amazon CloudWatch Log Groups. |
| 6.4 | cloud-trail-cloud-watch-logs-enabled | Use Amazon CloudWatch to centrally collect and manage log event activity. Inclusion of AWS CloudTrail data provides details of API call activity within your AWS account. |
| 6.4 | cloudtrail-enabled | AWS CloudTrail can help in non-repudiation by recording AWS Management Console actions and API calls. You can identify the users and AWS accounts that called an AWS service, the source IP address where the calls generated, and the timings of the calls. Details of captured data are seen within AWS CloudTrail Record Contents. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4 | cloud-trail-encryption-enabled | Because sensitive data may exist and to help protect data at rest, ensure encryption is enabled for your AWS CloudTrail trails. |
| 6.4 | cloud-trail-log-file-validation-enabled | Utilize AWS CloudTrail log file validation to check the integrity of CloudTrail logs. Log file validation helps determine if a log file was modified or deleted or unchanged after CloudTrail delivered it. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. |
| 6.4 | ec2-stopped-instance | Enable this rule to help with the baseline configuration of Amazon Elastic Compute Cloud (Amazon EC2) instances by checking whether Amazon EC2 instances have been stopped for more than the allowed number of days, according to your organization's standards. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.4 | vpc-flow-logs-enabled | The VPC flow logs provide detailed records for informati on about the IP traffic going to and from network interfaces in your Amazon Virtual Private Cloud (Amazon VPC). By default, the flow log record includes values for the different components of the IP flow, including the source, destination, and protocol. |
| 6.5A | guardduty-enabled-centraliz ed | Amazon GuardDuty can help to monitor and detect potential cybersecurity events by using threat intellige nce feeds. These include lists of malicious IPs and machine learning to identify unexpected, unauthorized, and malicious activity within your AWS Cloud environment. |

| Control ID | AWS Config Rule | Guidance |
| --- | --- | --- |
| 6.5A | securityhub-enabled | AWS Security Hub helps to monitor unauthorized personnel, connections, devices, and software. AWS Security Hub aggregates, organizes, and prioritizes the security alerts, or findings, from multiple AWS services. Some such services are Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer, and AWS Firewall Manager, and AWS Partner solutions. |

### Template

The template is available on GitHub: Operational Best Practices for SWIFT CSP.

## Security Best Practices for Amazon Elastic Container Service (Amazon ECS)

This conformance pack contains AWS Config rules based on Amazon ECS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon ECS.

## Security Best Practices for Amazon Elastic File System (Amazon EFS)

This conformance pack contains AWS Config rules based on Amazon EFS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon EFS.

## Security Best Practices for Amazon Elastic Kubernetes Service (Amazon EKS)

This conformance pack contains AWS Config rules based on Amazon EKS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon EKS.

## Security Best Practices for Amazon CloudFront

This conformance pack contains AWS Config rules based on Amazon CloudFront. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon CloudFront.

## Security Best Practices for Amazon OpenSearch Service

This conformance pack contains AWS Config rules based on Amazon OpenSearch Service. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon OpenSearch Service.

## Security Best Practices for Amazon Redshift

This conformance pack contains AWS Config rules based on Amazon Redshift. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon Redshift.

## Security Best Practices for Amazon Relational Database Service (Amazon RDS)

This conformance pack contains AWS Config rules based on Amazon RDS. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon RDS.

## Security Best Practices for AWS Auto Scaling

This conformance pack contains AWS Config rules based on AWS Auto Scaling. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for AWS Auto Scaling.

## Security Best Practices for AWS CloudTrail

This conformance pack contains AWS Config rules based on AWS CloudTrail. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for AWS CloudTrail.

## Security Best Practices for AWS CodeBuild

This conformance pack contains AWS Config rules based on AWS CodeBuild. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for AWS CodeBuild.

## Security Best Practices for Amazon ECR

This conformance pack contains AWS Config rules based on Amazon Elastic Container Registry (Amazon ECR). For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon ECR.

## Security Best Practices for AWS Lambda

This conformance pack contains AWS Config rules based on AWS Lambda. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for AWS Lambda.

## Security Best Practices for AWS Network Firewall

This conformance pack contains AWS Config rules based on AWS Network Firewall. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for AWS Network Firewall.

## Security Best Practices for Amazon SageMaker AI

This conformance pack contains AWS Config rules based on Amazon SageMaker AI. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for Amazon SageMaker AI.

## Security Best Practices for AWS Secrets Manager

This conformance pack contains AWS Config rules based on AWS Secrets Manager. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for AWS Secrets Manager.

## Security Best Practices for AWS WAF

This conformance pack contains AWS Config rules based on AWS WAF. For a list of all managed rules supported by AWS Config, see List of AWS Config Managed Rules.

See the `Parameters` section in the following template for the names and descriptions of the required parameters.

The template is available on GitHub: Security Best Practices for AWS WAF.

## Example Templates with Remediation Action

### Operational Best Practices For Amazon DynamoDB with Remediation

The template is available on GitHub: Operational Best Practices For Amazon DynamoDB with Remediation.

### Operational Best Practices For Amazon S3 with Remediation

The template is available on GitHub: Operational Best Practices For Amazon S3 with Remediation.

For more information about template structure, see Template Anatomy in the AWS CloudFormation User Guide.

# Creating templates for Custom Conformance Packs for AWS Config

A custom conformance pack is a unique collection of AWS Config rules and remediation actions that you can deploy together in an account and an AWS Region, or across an organization in AWS Organizations.

To make a custom conformance pack, follow the steps in the following **Customizing the template** section to author a YAML file that contains the list of AWS Config Managed Rules or AWS Config Custom Rules that you want to work with.

**Topics**


- Terminology
- Customizing the template


## Terminology

*AWS Config Managed Rules* are predefined rules owned by AWS Config.

*AWS Config Custom Rules* are rules that you create from scratch.

There are two ways to create AWS Config custom rules: with Lambda functions (AWS Lambda Developer Guide) and with Guard (Guard GitHub Repository), a policy-as-code language. AWS Config custom rules created with AWS Lambda are called *AWS Config Custom Lambda Rules* and AWS Config custom rules created with Guard are called *AWS Config Custom Policy Rules*.

## Customizing the template

### Creating your YAML file

To create a YAML file, open a text editor and save the file as *.yaml*.

> **Note**
>
> Your file will contain a **Parameters** and **Resources** section.

### Parameters

The `Parameters` section in your YAML file is for the rule parameters for the set of AWS Config rules that you will add later in the `Resources` section. Create the `Parameters` section by copying and pasting the following code block into your YAML file, customizing it as needed and repeating for each rule parameter.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

For example:

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> When selecting the AWS Config Rules to build your custom conformance pack, check you have the resources provisioned within your account that will be evaluated for the AWS Config Rules.

1. The first line in the parameter section after `Parameters:` is a concatenated string of *`NameOfRule`* + Param + *`NameOfRuleParameter`*.

   a. Replace *`NameOfRule`* with a consistent name that you create for the rule. For example, that could be **IamPasswordPolicy** for the **iam-password-policy** rule.

   b. Type `Param`.

   c. Then, replace *`NameOfRuleParameter`* with the name of the rule parameter for your specific rule. For AWS Config Managed Rules, the name of the rule parameter is located in the List of AWS Config Managed Rules (for example, **MinimumPasswordLength** is a name of a rule parameter for the **iam-password-policy** rule). For AWS Config Custom Rules, the name of the rule parameter is the name that you chose when you created the rule.

2. If you are using an AWS Config Managed Rule, find the appropriate AWS Config rule in the list of managed rules so you'll know the accepted values for `Default` and `Type` for your particular rule. For AWS Config Custom Rules, use the values you selected when creating your rule.

> **Note**
>
> For each parameter, `Type` must be specified. `Type` can be one of "String", "int", "double", "CSV", "boolean" and "StringMap".

### Resources

The `Resources` section lists the rules that are being added to your Custom Conformance Pack. Add the following `Resources` block directly beneath your `Parameters` section, customizing it as needed and repeating for each rule. For more information on the specifications, see AWS::Config::ConfigRule.

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: !Ref NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
     ...
```

For example:

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> When selecting the AWS Config rules to build your custom conformance pack, check that you have the resources that will be evaluated for the AWS Config rules provisioned within your account. For more information, see Supported Resource Types.

1. Replace *NameOfRule* with the same name you created in the `Parameters` section.
2. For AWS Config Managed Rules, replace *ActualConfigRuleName* with the title of the appropriate rule page on the List of AWS Config Managed Rules. For AWS Config Custom Rules, use the Config Rule name you chose at the time of the rule's creation.
3. Replace *NameOfRuleParameter* with the same name you used in the `Parameters` section. After the colon, copy and paste the same concatenated string of `!Ref` + *NameOfRule* + Param + *NameOfRuleParameter* that you created in `Parameters` section.
4. Change *Owner* to the appropriate value.

   > **Note**
   >
   > **AWS Config Managed Rules**
   > For AWS Config Managed Rules, the value for `Owner` will be `AWS`.
   > **AWS Config Custom Rules**
   > For AWS Config custom rules created with Guard, the value for `Owner` will be `CUSTOM_POLICY`. For AWS Config custom rules created with Lambda, the value for `Owner` will be `CUSTOM_LAMBDA`.

5. Change *SOURCE_IDENTIFIER* to the appropriate value.

   > **Note**
   >
   > **AWS Config Managed Rules**
   > For AWS Config Managed Rules, copy the identifier by following the link from the rule you select from the List of AWS Config Managed Rules (for example, the source identifier for the **access-keys-rotated** rule is **ACCESS_KEYS_ROTATED**).
   > **AWS Config Custom Rules**

For AWS Config custom rules created with Lambda, the `SourceIdentifier` is the Amazon Resource Name (ARN) of the rule's AWS Lambda function, such as `arn:aws:lambda:us-east-2:123456789012:function:`*`ActualConfigRuleName`*. For AWS Config custom rules created with Guard, this field is not needed.

Altogether, your filled out custom conformance pack should begin to look similar to the following, which is an example using these AWS Config Managed Rules: **iam-password-policy**, **access-keys-rotated**, and **iam-user-unused-credentials-check**.

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: !Ref AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
```

```
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge: !Ref
IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

# Deploying Conformance Packs for AWS Config

You can use the AWS Config console or the AWS CLI to deploy your conformance packs.

Deploy Conformance Packs (Console)

On the **Conformance packs** page, you can deploy a conformance pack for an account in a Region. You can also edit and delete the deployed conformance pack.

You can deploy a conformance pack using AWS Config sample templates or your own custom template. For instructions on how to create personalized conformance packs, see Custom Conformance Pack.

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the **Conformance packs** page and choose **Deploy conformance pack**.
3. On the **Specify template** page, either choose a sample template or use an existing template. For more information, see Conformance Pack Sample Templates.

   - If you choose **Use sample template**, select a **Sample template** from the dropdown list of sample templates.

     For information about the contents of each template, see Conformance Pack Sample Templates.
   - If you choose **Template is ready**, specify the template source. It is either an Amazon S3 URI, an AWS Systems Manager document (SSM document), or a template that you upload.

     If your template is more than 50 KB, upload it to the S3 bucket and select that S3 bucket location. For example: s3://*bucketname/prefix*.

> **Important**
>
> Choose **Template is ready** if you created your conformance pack YAML file from scratch based on Custom Conformance Pack.

4. Choose **Next**.
5. On the **Specify conformance pack details** page, enter the name for your conformance pack.

   The conformance pack name must be a unique name with a maximum of 256 alphanumeric characters. The name can contain hyphens but cannot contain spaces.
6. Optional: Add a parameter.

   Parameters are defined in your template and help you manage and organize your resources.
7. Choose **Next**.
8. On the **Review and deploy** page, review all of the information.

   You can edit the template details and conformance pack details by choosing **Edit**.
9. Choose **Deploy conformance pack**.

   AWS Config displays the conformance pack on the conformance pack page with the appropriate status.

   If your conformance pack deployment fails, check your permissions, verify that you did the prerequisite steps, and try again. Or you can contact AWS Support.

To deploy a **conformance pack using sample template with remediations**, see the A. Prerequisites for Using a Conformance Pack With Remediation and then use the preceding procedure.

To deploy a **conformance pack with one or more AWS Config rules**, see the B. Prerequisites for Using a Conformance Pack With One or More Custom AWS Config Rules.

Deploy Conformance Packs (AWS CLI)

1. Open a command prompt or a terminal window.

2. Enter one of the following commands to deploy a conformance pack named **`MyConformancePack`**. The template source is either an Amazon S3 URI, a template that you upload, or an AWS Systems Manager document (SSM document).

   **Amazon S3 URI**

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   **YAML template from your local directory**

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   **AWS Systems Manager Document (Systems Manager Document)**

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

3. Press Enter to run the command.

   You should see output similar to the following.

   ```
   {
       "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
   MyConformancePack1/conformance-pack-ID"
   }
   ```

> **Note**
>
> For more information on creating a YAML template for a conformance pack, see Custom Conformance Pack.

# Editing Conformance Packs for AWS Config

You can use the AWS Config console or the AWS CLI to edit your conformance packs.

Editing Conformance Packs (Console)

1. To edit a conformance pack, select the conformance pack from the table.
2. Choose **Actions** and then choose **Edit**.
3. On the **Edit conformance pack** page, you can edit the template details, sample template, conformance pack, and parameters section.

   You cannot change the name of the conformance pack.
4. Choose **Save changes**.

   The conformance pack is displayed with the AWS Config rules.

Editing Conformance Packs (AWS CLI)

If you are editing a conformance pack that you added previously, use the same `PutConformancePack` command that you use when deploying a conformance pack.

1. Open a command prompt or a terminal window.
2. Enter one of the following commands to deploy a conformance pack named **`MyConformancePack`**. The template source is either an Amazon S3 URI, a template that you upload, or an AWS Systems Manager document (SSM document).

   **Amazon S3 URI**

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   **YAML template from your local directory**

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

**AWS Systems Manager Document (Systems Manager Document)**

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket amzn-s3-demo-bucket
```

3. Press Enter to run the command.

   You should see output similar to the following.

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> For more information on creating a YAML template for a conformance pack, see Custom Conformance Pack.

# Deleting Conformance Packs for AWS Config

You can use the AWS Config console or the AWS CLI to delete conformance packs.

## Considerations

**Recommendation: Consider excluding the `AWS::Config::ResourceCompliance` resource type from recording before deleting rules**

Deleting rules creates configuration items (CIs) for `AWS::Config::ResourceCompliance` that can affect your costs for the configuration recorder. If you are deleting rules which evaluate a large number of resource types, this can lead to a spike in the number of CIs recorded.

To avoid the associated costs, you can opt to disable recording for the `AWS::Config::ResourceCompliance` resource type before deleting rules, and re-enable recording after the rules have been deleted.

However, since deleting rules is an asynchronous process, it might take an hour or more to complete. During the time when recording is disabled for `AWS::Config::ResourceCompliance`, rule evaluations will not be recorded in the associated resource's history.

## To delete a conformance pack

Deleting Conformance Packs (Console)

1. To delete a conformance pack, select the conformance pack from the table.
2. Choose **Actions** and then choose **Delete**.
3. On the delete *`conformance pack`* dialog box, confirm if you would like to permanently delete this conformance pack.

   > **Important**
   >
   > You cannot revert this action. When you delete a conformance pack, you delete all of the AWS Config rules and remediation actions in that conformance pack.

4. Enter **Delete** and choose **Delete**.

   On the **Conformance packs** page, you can see the deployment status as **Deleting** until the conformance pack is completely deleted.

Deleting Conformance Packs (AWS CLI)

Enter the following command.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

If successful, the command runs with no additional output.

> **Important**
>
> You cannot revert this action. When you delete a conformance pack, you delete all of the AWS Config rules and remediation actions in that conformance pack.

# Viewing Details and Compliance Information for your Conformance Packs for AWS Config

> **Important**
>
> For accurate reporting on the compliance status, you must record the `AWS::Config::ResourceCompliance` resource type. For more information, see Recording AWS Resources.

You can use the AWS Config console or the AWS CLI to view your conformance packs. The AWS Config console has a unified dashboard. The AWS CLI allows you to run commands for specific information.

Viewing Conformance Packs (Console)

To view your conformance packs in the AWS Management Console, see Conformance Pack Dashboard Pack.

Viewing the Details for your Conformance Packs (AWS CLI)

1. Enter the following command.

```
aws configservice describe-conformance-packs
```

OR

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. You should see output similar to the following.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

### Viewing the Status for your Conformance Packs (AWS CLI)

1. Enter the following command.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. You should see output similar to the following .

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

### Viewing the Compliance Status for your Conformance Packs (AWS CLI)

1. Enter the following command.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. You should see output similar to the following.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
```

```
        }
    ]
}
```

## Viewing the Compliance Details for your Conformance Packs (AWS CLI)

1. Enter the following command.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. You should see output similar to the following.

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
```

```
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

# Viewing the Compliance History Timeline for Conformance Packs for AWS Config

AWS Config supports storing compliance state changes to your conformance packs. This allows you to view the history of compliance state changes. These compliance state changes are presented as a timeline. The timeline captures changes as `ConfigurationItems` over a period of time. You can also use this feature to find specific rules within a conformance pack that are noncompliant.

You can opt in or out to record all resource types in AWS Config. If you have opted to record all resource types, AWS Config automatically begins recording the conformance pack compliance history as evaluated by AWS Config Rules. By default, AWS Config records the configuration changes for all supported resources. You can also select only the specific conformance pack compliance history resource type: `AWS::Config::ConformancePackCompliance`. Recording for the `AWS::Config::ConformancePackCompliance` resource type is available at no additional charge. For more information, see Recording AWS Resources.

A conformance pack is compliant if all of the rules in a conformance packs are compliant. It is noncompliant if any of the rules are not compliant. The compliance status of a conformance pack is INSUFFICIENT_DATA only if all rules within a conformance pack cannot be evaluated due to insufficient data. If some of the rules in a conformance pack are compliant but the compliance status of other rules in that same conformance pack is INSUFFICIENT_DATA, the conformance pack shows compliant. Compliance for a conformance pack is not evaluated all at one time. Some rules may take a longer time to evaluate than others. Compliance is evaluated for groups of rules at a time, continuing in stages until all the rules in a conformance pack have been evaluated.

## Viewing the Compliance Timeline

Access the compliance timeline by selecting a specific conformance pack from the **Conformance pack** main page.

1. Navigate to the **Conformance Pack** page.

2. On the **Conformance Pack** main page, choose a specific conformance pack and then choose **Conformance pack timeline** .

> **Note**
>
> Alternatively, you can use the compliance timeline from the conformance pack's details page. Choose a conformance pack and choose **View details** in the **Actions** dropdown. From this page, choose **Conformance pack timeline**.

The timeline shows you the history of compliance state changes for a conformance pack. You can do the following:

1. Expand a compliance change to view the line-by-line compliance status of each rule within a conformance pack.
2. From the expanded view, choose a specific rule to view its details page.

## Querying Compliance History for Conformance Packs for AWS Config

Query the compliance history using get-resource-config-history using the resource type `AWS::Config::ConformancePackCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

You should see output similar to the following:

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
```

```
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
```

```
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

For more information, see Supported Resource Types (AWS Config) and GetResourceConfigHistory in the API reference.

# Managing Conformance Packs for AWS Config Across all Accounts in Your Organization

Use AWS Config to manage conformance packs across all AWS accounts within an organization. You can do the following:

- Centrally deploy, update, and delete conformance packs across member accounts in an organization in AWS Organizations.
- Deploy a common set of AWS Config rules and remediation actions across all accounts and specify accounts where AWS Config rules and remediation actions should not be created.
- Use the management account in AWS Organizations to enforce governance by ensuring that the underlying AWS Config rules and remediation actions are not modifiable by your organization's member accounts.

## Considerations

### For deployments across different regions

The API call to deploy rules and conformance packs across accounts is AWS Region specific. At the organization level, you need to change the context of your API call to a different region if you want to deploy rules in other regions. For example, to deploy a rule in US East (N. Virginia), change the region to US East (N. Virginia) and then call `PutOrganizationConfigRule`.

### For accounts within an organization

If a new account joins an organization, the rule or conformance pack is deployed to that account. When an account leaves an organization, the rule or conformance pack is removed.

If you deploy an organizational rule or conformance pack in an organization administrator account, and then establish a delegated administrator and deploy an organizational rule or conformance pack in the delegated administrator account, you won't be able to see the organizational rule or conformance pack in the organization administrator account from the delegated administrator account or see the organizational rule or conformance pack in the delegated administrator account from organization administrator account. The DescribeOrganizationConfigRules and DescribeOrganizationConformancePacks APIs can only see and interact with the organization-related resource that were deployed from within the account calling those APIs.

**Retry mechanism for new accounts added to an organization**

Deployment of existing organizational rules and conformance packs will only be retried for 7 hours after an account is added to your organization if a recorder is not available. You are expected to create a recorder if one doesn't exist within 7 hours of adding an account to your organization.

**Organization management accounts, delegated administrators, and service-linked roles**

If you are using an organization management account and intend to use a delegated administrator for organizational deployment, be aware that AWS Config won't automatically create the service-linked role (SLR). You must manually create the service-linked role (SLR) separately using IAM.

If you do not have an SLR for your management account, you will not be able to deploy resources to that account from a delegated administrator account. You will still be able to deploy conformance packs to member accounts from management and delegated administrator accounts. For more information, see Using service-linked roles in the *AWS Identity and Access Management (IAM) User Guide*.

## Deployment

To deploy with the AWS Management Console

To a deploy a conformance pack across an organization from the AWS console, use AWS Systems Manager. For more information, see Deploy AWS Config conformance packs in the *AWS Systems Manager User Guide*.

To deploy with the AWS API

For information on how to integrate AWS Config with AWS Organizations, see AWS Config and AWS Organizations in the *AWS Organizations User Guide*. Ensure AWS Config recording is on before you use the following APIs to manage conformance pack rules across all AWS accounts within an organization:

- DeleteOrganizationConformancePack, deletes the specified organization conformance pack and all of the config rules and remediation actions from all member accounts in that organization.
- DescribeOrganizationConformancePacks, returns a list of organization conformance packs.
- DescribeOrganizationConformancePackStatuses, provides organization conformance pack deployment status for an organization.
- GetOrganizationConformancePackDetailedStatus, returns detailed status for each member account within an organization for a given organization conformance pack.
- PutOrganizationConformancePack, deploys conformance packs across member accounts in an AWS Organization.

## Region Support

Deploying conformance packs across member accounts in an AWS Organization is supported in the following Regions.

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS |
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS |

# Troubleshooting for Conformance Packs for AWS Config

Check the following issues to help troubleshoot issues you might run into when using conformance packs.

**Topics**


- Failed status for a conformance pack
- Dangling rules in a conformance pack


## Failed status for a conformance pack

If you get an error indicating that the conformance pack failed while creating, updating, or deleting it, you can check the status of your conformance pack.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

You should see output similar to the following.

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

Check the **ConformancePackStatusReason** for information about the failure.

**When the stackArn is present in the response**

If the error message is not clear or if the failure is due to an internal error, go to the CloudFormation console and do the following:

1. Search for the **stackArn** from the output.
2. Choose the **Events** tab of the CloudFormation stack and check for failed events.

   The status reason indicates why the conformance pack failed.

**When the stackArn is not present in the response**

If you receive a failure while you create a conformance pack but the stackArn is not present in the status response, the possible reason is that the stack creation failed and CloudFormation rolled back and deleted the stack. Go to the CloudFormation console and search for stacks that are in a **Deleted** state. The failed stack might be available there. The CloudFormation stack contains the conformance pack name. If you find the failed stack, choose the **Events** tab of the CloudFormation stack and check for failed events.

If none of these steps worked and if the failure reason is an internal service error, then try operation again or contact the AWS Support Center.

## Dangling rules in a conformance pack

Deploying a conformance pack involves the creation of an underlying AWS CloudFormation stack in the background to deploy the rules in the conformance pack template. These rules are service-linked rules and cannot be updated or deleted outside the conformance pack.

If you make changes to the underlying CloudFormation stack, this results in a situation where the conformance pack and its rules become unmanageable. These unmanageable rules are *dangling rules*.

### Drift between the CloudFormation stack and the conformance pack

You can update the rule names in a conformance pack template directly from the CloudFormation console. If you update the template directly from the CloudFormation console, this does not update the deployed conformance pack.

This drift creates a dangling rule. If you try to delete the rule from the conformance pack, you receive an error similiar to the following:

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

If you try to delete the conformance pack, the dangling rule cannot be deleted and you receive an error similiar to the following:

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

To fix this issue, do the following steps:

1. Delete the stack. For more information, see Deleting a stack on the CloudFormation console in the *CloudFormation User Guide*.
2. Delete the conformance pack using the AWS Config console or using the DeleteConformancePack API. If it is an organizational conformance pack and you are using the

management or delegated administrator account, use the DeleteOrganizationConformancePack API.

3. Reach out to the AWS Support Center with the Amazon Resource Name (ARN) of the dangling rules in the conformance pack to help clean up your account.

To avoid this issue, remember these best practices:

- Never make any direct updates to the CloudFormation stack of a conformance pack.
- Never try and make changes which create drift between the conformance pack and its underlying CloudFormation stack.
- The service-linked role (SLR) for conformance packs cannot be modified. Make sure the resources you are updating are part of the permissions policy for the SLR.

**Deleted CloudFormation stack for a conformance pack**

Unless there is drift between the CloudFormation stack and the conformance pack, it is never recommended to delete rules in a conformance pack or its CloudFormation stack directly from the CloudFormation console.

To fix this issue, reach out to the AWS Support Center with the Amazon Resource Name (ARN) of the dangling rules in the conformance pack to help clean up your account.

To avoid this issue, remember these best practices:

- Never delete the underlying CloudFormation stack for a conformance pack.
- Delete conformance packs using the DeleteConformancePack API. If it is an organizational conformance pack and you are using the management or delegated administrator account, use the DeleteOrganizationConformancePack API.

# Remediating Noncompliant Resources with AWS Config

AWS Config allows you to remediate noncompliant resources that are evaluated by AWS Config Rules. AWS Config applies remediation using AWS Systems Manager Automation documents. These documents define the actions to be performed on noncompliant AWS resources evaluated by AWS Config Rules. You can associate SSM documents by using AWS Management Console or by using APIs.

AWS Config provides a set of managed automation documents with remediation actions. You can also create and associate custom automation documents with AWS Config rules.

**Topics**


- Region Support
- Setting Up Manual Remediation for AWS Config
- Setting Up Auto Remediation for AWS Config
- Deleting Remediation Actions for AWS Config


## Region Support

Currently, remediation actions for AWS Config Rules is supported in the following regions:

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS |
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS | |

# Setting Up Manual Remediation for AWS Config

To apply remediation on noncompliant resources, you can either choose the remediation action you want to associate from a prepopulated list or create your own custom remediation actions using SSM documents. AWS Config provides a recommended list of remediation action in the AWS Management Console.

Setting Up Manual Remediation (Console)

In the AWS Management Console, you can either choose to manually remediate noncompliant resources by associating remediation actions with AWS Config rules. With all remediation actions, you can either choose manual or automatic remediation.

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Rules** on the left and then on the **Rules** page, choose **Add Rule** to add new rules to the rule list

   For existing rules, select the noncompliant rule from the rule list and choose the **Actions** dropdown list.
3. From the **Actions** dropdown list, choose **Manage remediation**. Select "Manual remediation" and then choose the appropriate remediation action from the recommended list.

> **Note**
>
> You can only manage remediations for non-service linked AWS Config rules. For more information, see Service-Linked AWS Rules.

Depending on the selected remediation action, you see specific parameters or no parameters.

4. (Optional): If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

   Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the dropdown list, you can enter values for each key. If you choose a resource ID parameter from the dropdown list, you can enter values for all the other keys except the selected resource ID parameter.

5. Choose **Save**. The **Rules** page is displayed.

For troubleshooting failed remediation actions, you can run the AWS Command Line Interface command `describe-remediation-execution-status` to get detailed view of a Remediation Execution for a set of resources. The details include state, timestamps for remediation execution steps, and any error messages for the failed steps.

Setting Up Manual Remediation (API)

Use the following AWS Config API operation to set up manual remediation:

- PutRemediationConfigurations, adds or updates the remediation configuration with a specific AWS Config rule with the selected target or action.
- StartRemediationExecution, runs an on-demand remediation for the specified AWS Config rules against the last known remediation configuration.
- DescribeRemediationExecutionStatus, provides a detailed view of a Remediation Execution for a set of resources including state, timestamps for when steps for the remediation execution occur, and any error messages for steps that have failed.
- DescribeRemediationConfigurations, returns the details of one or more remediation configurations.

# Setting Up Auto Remediation for AWS Config

To apply remediation on noncompliant resources, you can either choose the remediation action you want to associate from a prepopulated list or create your own custom remediation actions

using SSM documents. AWS Config provides a list of remediation action in the AWS Management Console.

Setting Up Auto Remediation (Console)

In the AWS Management Console, you can either choose to automatically remediate noncompliant resources by associating remediation actions with AWS Config rules. With all remediation actions, you can either choose manual or automatic remediation.

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Rules** on the left and then on the **Rules** page, choose **Add Rule** to add new rules to the rule list.

   For existing rules, select the noncompliant rule from the rule list and choose the **Actions** dropdown list.
3. From the **Actions** dropdown list, choose **Manage remediation**. Select "Automatic remediation" and then choose the appropriate remediation action from the list.

   > **Note**
   >
   > You can only manage remediations for non-service linked AWS Config rules. For more information, see Service-Linked AWS Rules.

   Depending on the selected remediation action, you see specific parameters or no parameters.
4. Choose **Auto remediation** to automatically remediate noncompliant resources.

   If a resource is still noncompliant after auto remediation, you can set the rule to try auto remediation again. Enter the desired retries and seconds.

   > **Note**
   >
   > There are costs associated with running a remediation script multiple times. Retries only occur if remediation fails and work within the specified time period; for example, 5 retries in 300 seconds. For more information, see Systems Manager Automation Pricing .

5. (Optional): If you want to pass the resource ID of noncompliant resources to the remediation action, choose **Resource ID parameter**. If selected, at runtime that parameter is substituted with the ID of the resource to be remediated.

   Each parameter has either a static value or a dynamic value. If you do not choose a specific resource ID parameter from the dropdown list, you can enter values for each key. If you choose a resource ID parameter from the dropdown list, you can enter values for all the other keys except the selected resource ID parameter.

6. Choose **Save**. The **Rules** page is displayed.

**For troubleshooting failed remediation actions**

For troubleshooting failed remediation actions, you can run the AWS Command Line Interface command `describe-remediation-execution-status` to get detailed view of a Remediation Execution for a set of resources. The details include state, timestamps for remediation execution steps, and any error messages for the failed steps.

**Auto remediation can be initiated even for compliant resources**

If you enable auto remediation for a specific AWS Config rule using the PutRemediationConfigurations API or the AWS Config console, it initiates the remediation process for all noncompliant resources for that specific rule. The auto remediation process relies on the compliance data snapshot which is captured on a periodic basis. Any noncompliant resource that is updated between the snapshot schedule will continue to be remediated based on the last known compliance data snapshot.

This means that in some cases auto remediation can be initiated even for compliant resources, since the bootstrap processor uses a database that can have stale evaluation results based on the last known compliance data snapshot.

Setting Up Auto Remediation (API)

Use the following AWS Config API operation to set up auto remediation:

- PutRemediationExceptions, adds a new exception or updates an existing exception for a specific resource with a specific AWS Config rule.
- DescribeRemediationExceptions, returns the details of one or more remediation exceptions.

# Deleting Remediation Actions for AWS Config

You can use the AWS Config console or the AWS CLI to delete remediation actions.

Deleting remediation actions (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Rules** on the left and then on the **Rules** page, select the rule from the rule list and choose **View details**.
3. On the *name of the rule* page, go to the **Remediation action** section. Expand the section to view additional details.
4. In the **Remediation action** section, choose **Delete** and confirm your delete action.

   > **Note**
   >
   > If remediation is in progress, a remediation action won't be deleted. Once you choose delete a remediation action, you cannot retrieve the remediation action. Deleting a remediation action does not delete the associated rule.

   If a remediation action is deleted, the **Resource ID parameter** will be empty and display N/A. On the **Rules** page, the remediation action column displays **Not set** for the associated rule.

Deleting remediation actions (API)

Use the following AWS Config API operation to set up auto remediation:

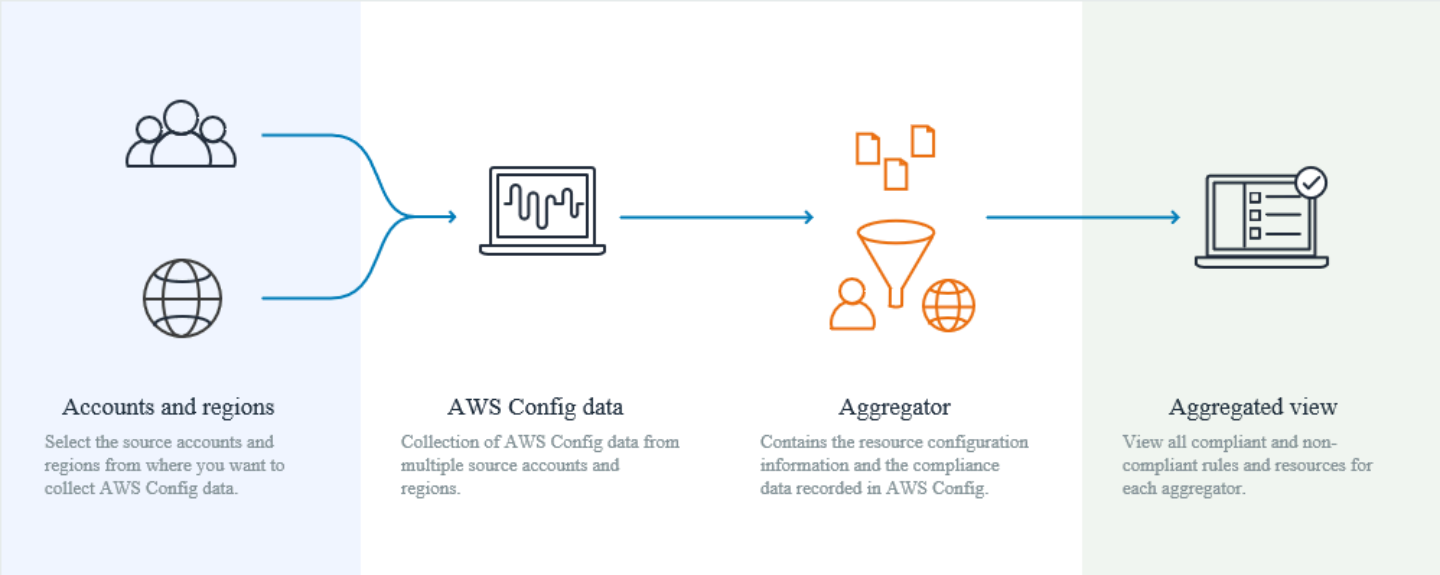
- DeleteRemediationConfiguration, deletes the remediation configuration.
- DeleteRemediationExceptions, deletes one or more remediation exceptions mentioned in the resource keys.

# Multi-Account Multi-Region Data Aggregation for AWS Config

An aggregator is an AWS Config resource type that collects AWS Config configuration and compliance data from the following:

- Multiple accounts and multiple AWS Regions.
- Single account and multiple AWS Regions.
- An organization in AWS Organizations and all the accounts in that organization which have AWS Config enabled.

Use an aggregator to view the resource configuration and compliance data recorded in AWS Config. The following image displays how an aggregator collects AWS Config data from multiple accounts and Regions.




## Use Cases

- **Compliance Monitoring**: You can aggregate compliance data to assess the overall compliance postures of your organization, or across accounts and Regions.
- **Change Tracking**: You can track changes to resources over time across your organization, or across accounts and Regions.

- **Resource Relationships**: You can analyze resource dependencies and relationships across your organization, or across accounts and Regions.

> **Note**
>
> Aggregators provide a *read-only view* into the source accounts and Regions that the aggregator is authorized to view by replicating data from the source accounts into the aggregator account. Aggregators do not provide mutating access into a source account or region. For example, this means that you cannot deploy rules through an aggregator or push snapshot files to a source account or region through an aggregator.
> Using aggregators does not incur any additional costs.

## Terminology

A *source account* is the AWS account from which you want to aggregate AWS Config resource configuration and compliance data. A source account can be an individual account or an organization in AWS Organizations. You can provide source accounts individually or you can retrieve them through AWS Organizations.

A *source region* is the AWS Region from which you want to aggregate AWS Config configuration and compliance data.

An *aggregator account* is an account where you create an aggregator.

*Authorization* refers to the permissions you grant to an aggregator account and region to collect your AWS Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of AWS Organizations.

A *service-linked aggregator* is linked to a specific AWS service. The configuration and compliance data in scope are set by the linked service.

## Region Support

Currently, multi-account multi-region data aggregation is supported in the following Regions:

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific (Hyderabad) | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| (Malaysia) | | | |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS | |
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS | |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS | |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS | |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS | |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS | |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS | |
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS | |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS | |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS | |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS | |

# Viewing Compliance and Inventory Data in the Aggregator Dashboard for AWS Config

The dashboard on the **Aggregators** page displays the configuration data of your aggregated AWS resources. It provides an overview of your rules, conformance packs, and their compliance states.

The dashboard provides the total resource count of AWS resources. The resource types and source accounts are ranked by the highest number of resources. It also provides a count of compliant and noncompliant rules and conformance packs. The noncompliant rules are ranked by highest number of noncompliant resources. The noncompliant conformance packs and source accounts are ranked by the highest number of noncompliant rules.

After setting up AWS Config, it starts aggregating data from the specified source accounts into an aggregator. It might take a few minutes for the compliance status of rules to display.

## Using the Aggregator Dashboard

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the **Aggregators** page. You can view:
   - Your rules and their compliance states.
   - Your conformance packs and their compliance states.
   - Your AWS resources and their configuration data.
3. Choose an aggregator from the dashboard. Filter through your aggregators by aggregator name. You can view the following widgets:
   - **Resource inventory**

View the top 10 resource types from the selected aggregator, in descending order by the resource count. Choose the total number of resources for the selected aggregator, displayed in parentheses after **Resource inventory**, to go to the aggregated **Resources** page, where you can view all the resources for an aggregator. Alternatively, choose a resource type in the widget to go to the aggregated **Resources** page, filtered using the specified resource type.

- **Accounts by resource count**

  View the top five accounts from the selected aggeregator in the descending order by the resource count. Choose an account in the widget to go to the **Resources** page, filtered using the specified account.

- **Noncompliant rules**

  View the top five noncompliant rules from the selected Aggregator, in descending order by the number of noncompliant resources. Choose a rule in the widget to go to the details page for the specified rule. Choose **View all noncompliant rules** to go to the aggregated **Rules** page, where you can view all the rules for an aggregator.

- **Accounts by noncompliant rules**

  View the top five accounts from the selected aggregator, in descending order by the number of noncompliant rules. Choose an account in the widget to go to the aggregated **Rules** page, where you can view all the rules for an aggregator filtered using the specified account.

- **Accounts by noncompliant conformance packs**

  View the top five accounts from the selected aggregagtor, in descending order by the number of noncompliant conformance packs. Choose an account in the widget to go to the aggregated **Conformance Pack** page, where you can view all conformance packs for an aggregagtor filtered using the specified account.

4. In the left navigation pane, choose one of the following options from the dropdown menu:

   - **Compliance dashboard**

     View automated compliance dashboards by using the widgets that summarize insights about resource compliance within your aggregator. You can see data such as the top 10 resource types by noncompliant resources, and top 10 account level conformance packs by noncompliant rules. For information about these graphs and charts, see Compliance dashboards.

   - **Conformance packs**

View all conformance packs that are created and linked to the different AWS accounts within your aggregator. The **Conformance Pack** page displays a table that lists the name, Region, account ID, and compliance status of each conformance pack. From this page, you can choose a conformance pack and **View details** for more information about its rules and resources and their compliance status.

- **Rules**

  View all rules that are created and linked to the different AWS accounts within your aggregator. The **Rules** page displays a table that lists the name, compliance status, Region, and account of each rule. From this page, you can choose a rule and **View details** for information, such as its aggregator, Region, account ID, and resources in scope.

- **Inventory dashboard**

  View automated inventory dashboards by using the widgets that summarize insights about resource configuration data within your aggregator. You can see data such as the top 10 resource types by resource count, and the top 10 accounts by resource count. For information about these graphs and charts, see Inventory dashboards.

- **Resources**

  View all resources that are recorded and linked to the different AWS accounts within your aggregator. From the **Resource** page, choose a resource and **View details** to view its details, the rules associated with it, and the current resource configuration. You can also see information about the resource, such as its aggregator, Region, account ID, resource name, resource type, and resource ID.

- **Authorizations**

  View and manage all accounts currently authorized or pending authorization. From the **Authorizations** page, choose **Add authorization** to provide access to another account. Choose **Delete authorization** to revoke access from an account ID.

> **Note**
>
> **Troubleshooting**
>
> You might see the **Data collection from all source accounts and regions is incomplete** message displayed in the aggregated view for the following reasons:

- The transfer of noncompliant AWS Config rules and configuration data of AWS resources is in progress.
- AWS Config can't find rules to match the filter that you applied. Select the appropriate account or Region, and try again.

You might see this message display in the aggregated view: **Data collection from your organization is incomplete. You can view the below data only for 24 hours.** It displays for the following reasons:

- AWS Config can't access your organization details because of an IAM role that is not valid. If the IAM role remains not valid for more than 24 hours, AWS Config deletes the data for the entire organization.
- AWS Config service access is disabled in your organization.

## Compliance Dashboard

View automated compliance dashboards by using widgets that summarize insights about resource compliance within your aggregator This dashboard displays only rules with compliance results.

**Note**

**Limitations**

The insights in the compliance dashboard are provided by the Advanced Queries feature of AWS Config, and this feature does not support nested structures or unpacking nested arrays. This means that the compliance dashboard displays the overall compliance of a resource and not the compliance status for each specific rule which reports on a resource. For example, if you check the configuration item (CI) for the resource type `AWS::Config::ResourceCompliance`, the dashboard will display the compliance results for all the rules that report on that resource. If there are 10 rules that report on the resource, 9 of them are COMPLIANT, and only 1 is NON_COMPLIANT, the overall compliance of that resource will be NON_COMPLIANT.

**Compliance Summary By Resources**

Displays a pie chart comparing the number of compliant resources to noncompliant resources from the selected aggregator. Hover over the chart to see the exact number and percentage of compliant and noncompliant resources.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

**Top 10 resource types by noncompliant resources**

Displays a horizontal bar graph comparing up to 10 resource types from the selected aggregator in descending order by the number of noncompliant resources. Hover over the graph to see the exact number of noncompliant resources for each resource type.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

**Top 10 accounts by noncompliant resources**

*Top 10 accounts by noncompliant resources* displays a horizontal bar graph comparing up to 10 accounts from the selected aggregator in descending order by the number of noncompliant resources. Hover over the graph to see the exact number of noncompliant resources for each account.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

**Top 10 regions by noncompliant resources**

Displays a horizontal bar graph comparing up to 10 Regions where the selected aggregator collects data in descending order by the number of noncompliant resources. Hover over the graph to see the exact number of noncompliant resources for each Region.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator.

**Top 10 account level conformance packs by noncompliant rules**

Displays a horizontal bar graph comparing up to 10 account level conformance packs from the selected aggregator in descending order by the number of noncompliant rules. Hover over

the graph to see the percentage of compliant and noncompliant rules for each account level conformance pack.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

**Top 10 organization level conformance packs by noncompliant rules**

Displays a horizontal bar graph comparing up to 10 organizational level conformance packs from the selected aggregator in descending order by the number of noncompliant rules. Hover over the graph to see the percentage of compliant and noncompliant rules in each organizational level conformance pack.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

**Top 10 accounts by noncompliant rules across conformance packs**

*Top 10 accounts by noncompliant rules across conformance packs* displays a horizontal bar graph comparing up to 10 accounts from the selected aggregator in descending order by the number of noncompliant rules across all your conformance packs. Hover over the graph to see the exact number of noncompliant rules in each account.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

## Inventory Dashboard

View automated inventory dashboards by using widgets that summarize insights about resource configuration data within your aggregator.

**Top 10 resource types by resource count**

Displays a horizontal bar graph comparing up to 10 resource types from the selected aggregator in descending order by resource count. Hover over the graph to see the exact number of resources for each resource type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data.

**Resource count by region**

Displays a horizontal bar graph comparing up to 10 Regions where the selected aggregator collects data in descending order by resource count. Hover over the graph to see the exact number of resources for each Region.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator.

**Top 10 accounts by resource count**

Displays a horizontal bar graph comparing up to 10 accounts from the selected aggregator in descending order by resource count. Hover over the graph to see the exact number resources for each resource type.

The data displayed is dependent on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data.

**Resource count by Amazon EC2 service resource types**

Displays a horizontal bar graph comparing Amazon EC2 resource types from the selected aggregator in descending order by resource count. Hover over the graph to see the exact number of resources for each Amazon EC2 resource type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator, and the Regions where the selected aggregator is configured to collect data. To use this chart, you must configure the recorder to record Amazon EC2 resource types. For more information, see Selecting Which Resources AWS Config Records.

**Top 10 EC2 instance types used**

Displays a horizontal bar graph comparing up to 10 Amazon EC2 instance types from the selected aggregator in descending order by usage. Hover over the graph to see usage for each EC2 instance type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect

data. To use this chart, you must configure the recorder to record the EC2 instance resource type. For more information, see Recoding AWS Resources.

**EBS Volume counts by volume type and size**

Displays a vertical bar graph comparing EBS volumes from the selected aggregator by resource count. Hover over the graph to see the count and size breakdown for each type of EBS volume.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data. To use this chart, you must configure the recorder to record the EC2 volume resource type. For more information, see Selecting Which Resources AWS Config Records.

**Number of EC2 instances that are running vs. stopped by type**

Displays a horizontal bar graph comparing EC2 instance types from the selected aggregator that are running to EC2 instances that are stopped by instance type. Hover over the graph to see the exact number of stopped and running EC2 instances for each type.

The data displayed depends on the settings of the configuration recorder for each account in the selected aggregator and the Regions where the selected aggregator is configured to collect data. To use this chart, you must configure the recorder to record the EC2 instance resource type. For more information, see Recoding AWS Resources.

# Creating Aggregators for AWS Config

You can use the AWS Config console or the AWS CLI to create your aggregators. From the AWS Config you can choose **Add individual account IDs** or **Add my organization** from where you want to aggregate data. For the AWS CLI there are two different procedures.

Creating Aggregators (Console)

On the **Aggregator** page, you can create an aggregator by specifying the source account IDs or organization and regions from where you want to aggregate data.

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the **Aggregators** page and choose **Create aggregator**.
3. **Allow data replication**, gives permission to AWS Config to replicate data from the source accounts into an aggregator account.

Choose **Allow AWS Config to replicate data from source account(s) into an aggregator account. You must select this checkbox to continue to add an aggregator**.

4. For **Aggregator name**, type the name for your aggregator.

   The aggregator name must be a unique name with a maximum of 64 alphanumeric characters. The name can contain hyphens and underscores.

5. For **Select source accounts**, either choose **Add individual account IDs** or **Add my organization** from where you want to aggregate data.

   > **Note**
   >
   > Authorization is required when using **Add individual account IDs** to select source accounts.

   - If you choose **Add individual account IDs**, you can add individual account IDs for an aggregator account.
     1. Choose **Add source accounts** to add account IDs.
     2. Choose **Add AWS account IDs** to manually add comma-separated AWS account IDs. If you want to aggregate data from the current account, type the account ID of the account.

        OR

        Choose **Upload a file** to upload a file (.txt or .csv) of comma-separated AWS account IDs.
     3. Choose **Add source accounts** to confirm your selection.
   - If you choose **Add my organization**, you can add all accounts in your organization to an aggregator account.

     > **Note**
     >
     > You must be signed in to the management account or a registered delegated administrator and all the features must be enabled in your organization. If the caller is a management account, AWS Config calls `EnableAwsServiceAccess` API to enable integration between AWS Config and AWS Organizations.

If the caller is a registered delegated administrator, AWS Config calls `ListDelegatedAdministrators` API to verify whether the caller is a valid delegated administrator.
Ensure that the management account registers delegated administrator for AWS Config service principal name (config.amazonaws.com) before the delegated administrator creates an aggregator. To register a delegated administrator, see Registering a Delegated Administrator for AWS Config.

You must assign an IAM role to allow AWS Config to call read-only APIs for your organization.

1. Choose **Choose a role from your account** to select an existing IAM role.

> **Note**
>
> In the IAM console, attach the `AWSConfigRoleForOrganizations` managed policy to your IAM role. Attaching this policy allows AWS Config to call AWS Organizations `DescribeOrganization`, `ListAWSServiceAccessForOrganization`, and `ListAccounts` APIs. By default `config.amazonaws.com` is automatically specified as a trusted entity.

2. Or, choose **Create a role** and type a name for your IAM role name to create IAM role.

6. For **Regions**, choose the regions for which you want to aggregate data.
   - Select one region or multiple regions or all the AWS Regions.
   - Select **Include future AWS Regions** to aggregate data from all future AWS Regions where multi-account multi-region data aggregation is enabled.
7. Choose **Save**. AWS Config displays the aggregator.

Creating Aggregators using Individual Accounts (AWS CLI)

1. Open a command prompt or a terminal window.
2. Enter the following command to create an aggregator named **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

For `account-aggregation-sources`, enter one of the following.

- A comma-separated list of AWS account IDs for which you want to aggregate data. Wrap the account IDs in square brackets, and be sure to escape quotation marks (for example, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"], \"AllAwsRegions\": true}]"`).
- You can also upload a JSON file of comma-separated AWS account IDs. Upload the file using the following syntax: `--account-aggregation-sources MyFilePath/MyFile.json`

  The JSON file must be in the following format:

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Press Enter to execute the command.

   You should see output similar to the following:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
```

```
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

## Creating Aggregators using AWS Organizations (AWS CLI)

Before you begin this procedure, you must be signed in to the management account or a registered delegated administrator and all the features must be enabled in your organization.

> **Note**
>
> Ensure that the management account registers a delegated administrator with both of the following AWS Config service principal names (`config.amazonaws.com` and`config-multiaccountsetup.amazonaws.com`) before the delegated administrator creates an aggregator. To register a delegated administrator, see Registering a Delegated Administrator for AWS Config.

1. Open a command prompt or a terminal window.
2. If have not created an IAM role for your AWS Config aggregator, enter the following command:

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":\"\",\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action
\":\"sts:AssumeRole\"}]}" --description "Role for organizational AWS Config
 aggregator"
```

> **Note**
>
> Copy the Amazon Resource Name (ARN) from this IAM role for use when you create your AWS Config aggregator. You can find the ARN on the response object.

3. If have not attached a policy to your IAM role, attach the AWSConfigRoleForOrganizations managed policy or enter the following command:

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17",       "Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAW
```

4. Enter the following command to create an aggregator named **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Press Enter to execute the command.

   You should see output similar to the following:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

# Registering a Delegated Administrator for AWS Config

Delegated administrators are accounts within a given AWS Organization that are granted additional administrative privileges for a specified AWS service. For more information, see Delegated administrator in the *AWS Organizations User Guide*. You must use the AWS CLI to register a delegated administrator.

### Registering a Delegated Administrator

1. Log in with management account credentials.
2. Open a command prompt or a terminal window.
3. Enter the following command to enable service access as a delegated administrator for your organization to deploy and manage AWS Config rules and conformance packs across your organization:

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. Enter the following command to enable service access as a delegated administrator for your organization to aggregate AWS Config data across your organization:

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. To check if the enable service access is complete, enter the following command and press Enter to execute the command.

```
aws organizations list-aws-service-access-for-organization
```

You should see output similar to the following:

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
```

```
    ]
}
```

6. Next, enter the following command to register a member account as a delegated administrator for AWS Config.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. To check if the registration of delegated administrator is complete, enter the following command from the management account and press Enter to execute the command.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

You should see output similar to the following:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
```

```
}
```

# Editing Aggregators for AWS Config

You can use the AWS Config console or the AWS CLI to edit your aggregators.

Editing Aggregators (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the **Aggregator** page, and choose the aggregator name.
3. Choose **Actions** and then choose **Edit**.
4. Use the sections on the **Edit aggregator** page to change the source accounts, IAM roles, or regions for the aggregator.

   > **Note**
   >
   > You cannot change source type from individual account(s) to organization and vice versa.

5. Choose **Save**.

Editing Aggregators (AWS CLI)

1. You can use the `put-configuration-aggregator` command to update or edit a configuration aggregator.

   Enter the following command to add a new account ID to **`MyAggregator`**:

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. Depending on your source account you should see output similar to the following:

   **For individuals accounts**

   ```
   {
   ```

```
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

OR

### For an organization

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

# Deleting Aggregators for AWS Config

You can use the AWS Config console or the AWS CLI to delete your aggregators.

Deleting Aggregators (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the **Aggregator** page, and choose the aggregator name.
3. Choose **Actions** and then choose **Delete**.

   A warning message is displayed. Deleting an aggregator results in the loss of all aggregated data. You cannot recover this data but data in the source account(s) is not impacted.
4. Choose **Delete** to confirm your selection.

Deleting Aggregators (AWS CLI)

Enter the following command:

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

If successful, the command executes with no additional output.

# Authorizing Aggregator Accounts to Collect AWS Config Configuration and Compliance Data

*Authorization* refers to the permissions you grant to an aggregator account and region to collect your AWS Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of AWS Organizations. You can use the AWS Config console or the AWS CLI to authorize aggregator accounts.

**Topics**


- Considerations
- Adding Authorization

## Considerations

**There are two types of aggregators: Individual account aggregator and Organization aggregator**

For an individual account aggregator, authorization is required for all source accounts and Regions that you want to include, including both external accounts and Regions and Organization member accounts and Regions.

For an organization aggregator, authorization is not required for Organization member account regions since authorization is integrated with the AWS Organizations service.

**Aggregators do not automatically enable AWS Config on your behalf**

AWS Config needs to be enabled in the source account and Region for either type of aggregator, in order for AWS Config data to be generated in the source account and Region.

## Adding Authorization

Adding Authorization (Console)

You can add authorization to grant permission to aggregator accounts and Regions to collect AWS Config configuration and compliance data.

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Navigate to the **Authorizations** page and choose **Add authorization**.
3. For **Aggregator account**, type the 12-digit account ID of an aggregator account.
4. For **Aggregator region**, choose the AWS Regions where the aggregator account is allowed to collect AWS Config configuration and compliance data.
5. Choose **Add authorization** to confirm your selection.

   AWS Config displays an aggregator account, Region, and authorization status.

   > **Note**
   >
   > You can also add authorizations to aggregator accounts and Regions programatically using CloudFormation sample templates. For more information, see AWS::Config::AggregationAuthorization in the *CloudFormation User Guide*.

Authorizing a Pending Request (Console)

If you have a pending authorization request from an existing aggregator account you will see the request status on the **Authorizations** page. You can authorize a pending request from this page.

1. Choose the aggregator account that you want to authorize, and then choose **Authorize**.

   A confirmation message is displayed to confirm that you want to grant the aggregator account permission to collect AWS Config data from this account.
2. Choose **Authorize** again to confirm that you want to grant permission to the aggregator account.

   The authorization status changes from **Requesting for authorization** to **Authorized**.

**Authorization approval period**

Authorization approval is required to add source accounts to an individual account aggregator. A pending authorization approval request will be available for 7 days after an individual account aggregator adds a source account.

Adding Authorization (AWS CLI)

1. Open a command prompt or a terminal window.
2. Enter the following command:

```
aws configservice put-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

3. You should see output similar to the following:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

# Deleting Authorization for Aggregator Accounts to Collect AWS Config Configuration and Compliance Data

*Authorization* refers to the permissions you grant to an aggregator account and region to collect your AWS Config configuration and compliance data. Authorization is not required if you are aggregating source accounts that are part of AWS Organizations. You can use the AWS Config console or the AWS CLI to delete authorizations.

**Topics**


- Considerations
- Deleting Authorization


## Considerations

**There are two types of aggregators: Individual account aggregator and Organization aggregator**

For an individual account aggregator, authorization is required for all source accounts and Regions that you want to include, including both external accounts and Regions and Organization member accounts and Regions.

For an organization aggregator, authorization is not required for Organization member account regions since authorization is integrated with the AWS Organizations service.

**Aggregators do not automatically enable AWS Config on your behalf**

AWS Config needs to be enabled in the source account and Region for either type of aggregator, in order for AWS Config data to be generated in the source account and Region.

## Deleting Authorization

Deleting Authorization (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose the aggregator account that you want to delete authorization, and then choose **Delete**.

A warning message is displayed. When you delete this authorization, AWS Config data will no longer be shared with the aggregator account.

3. Choose **Delete** again to confirm your selection.

   The aggregator account is now deleted.

Deleting Authorization (AWS CLI)

Enter the following command:

```
aws configservice delete-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

If successful, the command executes with no additional output.

# Viewing Aggregators for AWS Config

You can use the AWS Config console or the AWS CLI to view your aggregators.

Viewing Aggregators (Console)

To view your conformance packs in the AWS Management Console, see Aggregator Dashboard.

Viewing Aggregators (AWS CLI)

1. Enter the following command:

   ```
   aws configservice describe-configuration-aggregators
   ```

2. Depending on your source account you should see output similar to the following:

   **For individuals accounts**

   ```
   {
       "ConfigurationAggregators": [
           {
               "ConfigurationAggregatorArn":
    "arn:aws:config:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
               "CreationTime": 1517942461.442,
   ```

```
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

OR

**For an organization**

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

# Troubleshooting for Multi-Account Multi-Region Data Aggregation for AWS Config

AWS Config might not aggregate data from source accounts for one of the following reasons:

| If this happens | Do this |
| --- | --- |
| AWS Config is not enabled in the source account for accounts within an Organization. | Enable AWS Config in the source account and authorize the aggregator account to collect data. |
| Authorization is not granted to an aggregator account. | Sign in to the source account and grant authorization to the aggregator account to collect AWS Config data. |
| There might be a temporary issue that is preventing data aggregation. | Data aggregation is subject to delays. Wait for a few minutes. |

AWS Config might not aggregate data from an organization for one of the following reasons:

| If this happens | Do this |
| --- | --- |
| AWS Config is unable to access your organization details due to invalid IAM role. | Create an IAM role or select a valid IAM role from the IAM role list.<br><br>**Note**<br>If the IAM role is invalid for more than 7 days, AWS Config deletes data for entire organizat ion. |
| AWS Config service access is disabled in your organization. | You can enable integration between AWS Config and AWS Organizations through the `EnableAWS ServiceAccess` API. If you choose **Add my organization** in console, AWS Config automatically enables the integration between AWS Config and AWS Organizations. |
| AWS Config is unable to access your organization details because all features is not enabled in your organization. | Enable all features in AWS Organizations console. |

| If this happens | Do this |
| --- | --- |
| Organizational changes such as adding an account, removing an account, enabling service access, and disabling service access are not updated in Middle East (Bahrain) and Asia Pacific (Hong Kong) regions immediately. | Organizational changes are subject to 2 hour delay. Wait for 2 hours to see all organization changes. |

# Querying the Current Configuration State of AWS Resources with AWS Config

Introducing a preview feature for advanced queries that allows you to use generative artificial intelligence (generative AI) capabilities to enter prompts in plain English and convert them into a ready-to-use query format. For more information, see Natural language query processor for advanced queries.

You can use AWS Config to query the current configuration state of AWS resources based on configuration properties for a single account and Region or across multiple accounts and Regions. You can perform property-based queries against current AWS resource state metadata across a list of resources that AWS Config supports. For more information on the list of supported resource types, see Supported Resource Types for Advanced Queries.

*Advanced queries* provides a single query endpoint and a query language to get current resource state metadata without performing service-specific describe API calls. You can use configuration aggregators to run the same queries from a central account across multiple accounts and AWS Regions.

**Topics**


- Features
- Query Components for AWS Config
- Query Using the SQL Query Editor for AWS Config (Console)
- Query Using the SQL Query Editor for AWS Config (AWS CLI)
- Natural language query processor for AWS Config advanced queries
- Example Queries for AWS Config
- Example Relationship Queries for AWS Config
- Limitations
- CIDR notation/IP range behavior for advanced queries
- Multiple properties within an array behavior for advanced queries
- Region Support

# Features

AWS Config uses a subset of structured query language (SQL) `SELECT` syntax to perform property-based queries and aggregations on the current configuration item (CI) data. The queries range in complexity from matches against tag and/or resource identifiers, to more complex queries, such as viewing all Amazon S3 buckets that have versioning disabled. This allows you to query exactly the current resource state you need without performing AWS service-specific API calls.

It supports aggregation functions such as `AVG`, `COUNT`, `MAX`, `MIN`, and `SUM`.

You can use advanced query for:

- Inventory management; for example, to retrieve a list of Amazon EC2 instances of a particular size.
- Security and operational intelligence; for example, to retrieve a list of resources that have a specific configuration property enabled or disabled.
- Cost optimization; for example, to identify a list of Amazon EBS volumes that are not attached to any EC2 instance.
- Compliance data; for example, to retrieve a list of all your conformance packs and their compliance status.

For information about how to use the AWS SQL Query Language, see [What Is SQL (Structured Query Language)?](#).

# Query Components for AWS Config

The SQL `SELECT` query components for AWS Config advanced queries are as follows.

## Synopsis

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

## Parameters

### [ WHERE condition ]

Filters results according to the `condition` you specify.

**Comparison operators**

- = (equals)
- `IN` (list membership)
- `BETWEEN` (range check)

**Logic operators**

- `AND`
- `OR`
- `NOT`

### [ GROUP BY property ]

Aggregates the result set into groups of rows with matching values for the given property.

The GROUP BY clause is applicable to aggregations.

### [ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]

Sorts a result set by one or more output `properties`.

When the clause contains multiple properties, the result set is sorted according to the first `property`, then according to the second `property` for rows that have matching values for the first property, and so on.

## Examples

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

# Query Using the SQL Query Editor for AWS Config (Console)

Introducing a preview feature for advanced queries that allows you to use generative artificial intelligence (generative AI) capabilities to enter prompts in plain English and convert them into a ready-to-use query format. For more information, see Natural language query processor for advanced queries.

You can either use AWS sample queries or you can create your own query called as custom queries.

## Considerations

### Prerequisites

If you are using the one of the following AWS managed policies, you will have the necessary permissions to run and save a query: AWSServiceRoleForConfig (service-linked role) or AWS_ConfigRole.

Otherwise, you must have the permissions included in the AWSConfigUserAccess AWS managed policy.

### List of properties that you can query

An updated list of properties and their data types is available in GitHub.

### Advanced queries and aggregators

To run a query on an aggregator, create an aggregator. For more information, see Creating Aggregators for AWS Config.

If you already have an aggregator set up, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the AWS account ID and AWS Region in the query statement to view that information in the results.

## Use an AWS Sample Query

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.

2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.
3. On the **Advanced queries** page, choose an appropriate query from the list of queries. You can filter through the list of queries either by the name, description, creator, or tags. To filter for AWS queries, choose **Creator**, and enter **AWS**. The query that you select is displayed in the SQL query editor. You can edit the selected query to fit your needs.
4. To save this query to a new query, choose **Save As**.
   - In the **Query Name** field, update the name of the query.
   - In the **Description** field, update the description of the query.
   - Enter up to 50 unique tags for this query.
   - Choose **Save**.
5. Choose **Run**. The query results are displayed in the table below the query editor.
6. Choose **Export as** to export the query results in CSV or JSON format.

## Create your custom query

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.
3. To create your custom query, choose **New query**.

   To view or edit a custom query, filter a query either by the name, description, creator or tags. To filter custom queries, choose **Creater** and enter **Custom**.
4. On the **Query editor** page, create your own query for this account and Region. You can also select an appropriate aggregator to create a query for multiple accounts and Regions.
5. Edit if you wish you make changes to this query. Choose **Save Query** to save this query.
   - In the **Query Name** field, update the name of the query.
   - In the **Description** field, update the description of the query.
   - Enter up to 50 unique tags for this query.
   - Choose **Save**.
6. Choose **Run**. The query results are displayed in the table below the query editor.

7. Choose **Export as** to export the query results in CSV or JSON format.

# Query Using the SQL Query Editor for AWS Config (AWS CLI)

The AWS CLI is a unified tool to manage your AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and use scripts to automate them. For more information about the AWS CLI and for instructions on installing the AWS CLI tools, see the following in the *AWS Command Line Interface User Guide*.

- AWS Command Line Interface User Guide
- Getting Set Up with the AWS Command Line Interface

If necessary, enter `aws configure` to configure the AWS CLI to use an AWS Region where advanced queries are available.

## Considerations

### Prerequisites

If you are using the one of the following AWS managed policies, you will have the necessary permissions to run and save a query: AWSServiceRoleForConfig (service-linked role) or AWS_ConfigRole.

Otherwise, you must have the permissions included in the AWSConfigUserAccess AWS managed policy.

### List of properties that you can query

An updated list of properties and their data types is available in GitHub.

### Advanced queries and aggregators

To run a query on an aggregator, create an aggregator. For more information, see Creating Aggregators for AWS Config.

If you already have an aggregator set up, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the AWS account ID and AWS Region in the query statement to view that information in the results.

# Query Resource Configuration Data

### To query your resource configuration data using the query editor (AWS CLI) for a single account and Region

1. Open a command prompt or a terminal window.
2. Enter the following command to query your resource configuration data.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

Depending on your query, the output looks like the following.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

### To query your resource configuration data using the query editor (AWS CLI) for multiple accounts and Regions

1. Open a command prompt or a terminal window.
2. Enter the following command to query your resource configuration data.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

Depending on your query, the output looks like the following.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> While using the `AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, and `AWS::IAM::Policy` resource types in an advanced query, use `awsRegion = 'global'`.

## Save a Query

1. Open a command prompt or a terminal window.
2. Enter the following command to save a query.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
```

```
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. Depending on your query, the output looks like the following.

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` is optional. When you pass the tags, the saved tags will not be returned by either `list-stored-queries` or `get-stored-query`. You must use `list-tag-for-resources` to retrieve the associated tags for a saved query.
> `--description` is optional while creating or updating a query.

## View all the Saved Queries

1. Enter the following command to view the list of all saved queries.

```
aws configservice list-stored-queries
```

2. Depending on your query, the output looks like the following.

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
```

```
    ]
}
}
```

## Get Details of a Saved Query

1. Enter the following command to get details of a specific saved query.

```
aws configservice get-stored-query --query-name cli-test
```

2. Depending on your query, the output looks like the following.

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

## Delete a Saved Query

- Enter the following command to delete your saved query.

```
aws configservice delete-stored-query --query-name cli-test
```

If successful, the command runs with no additional output.

# Natural language query processor for AWS Config advanced queries

> **Note**
>
> The public preview of AWS Config Natural Language Query Processor will be discontinued by January 15, 2026. Additionally, you can chat about your AWS resources using natural language prompts with Amazon Q Developer. For more information, see Chatting about your resources with Amazon Q Developer.

The natural language query processor for advanced queries uses Amazon Bedrock, a generative artificial intelligence (generative AI) technology which allows you to enter prompts in plain English and convert them into a ready-to-use query format. With the natural language query processor, you can query your AWS account or across an AWS organization.

A prompt can be a question or a statement. For example, you can enter prompts such as "Which load balancers are created after January 1, 2024?" and “List all my lambda function that is running node js 16.”

## Considerations

The natural language query processor cannot do the following actions:

- Generate queries from languages other than English.
- Generate queries from prompts that do not relate to advanced queries.
- Generate queries from prompts with more than 1000 characters.
- Generate queries from follow-up corrections or from previous sessions.
- Explain code that has been generated.

## Query using the natural language query processor

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Advanced queries** from the left navigation to query your resource configurations for a single account and Region or for multiple accounts and Regions.

3. On the **Advanced queries** page, choose **New query** to go to the Query editor.
   - (Optional) To run a query on an aggregator, create an aggregator. For more information, see Creating Aggregators for AWS Config.
   - If you've already set up an aggregator, in the query scope, choose the aggregator to run an advanced query on that aggregator. When you select an aggregator, consider adding the AWS account ID and AWS Region in the query statement to view that information in the results.
4. In the Query editor, go to the **Natural language query processor** section. Enter a prompt in plain English, and then choose **Generate**. For examples, see Example prompts.
5. After you generate a query, you can choose **Copy** (functionally equivalent to Ctrl+C) to copy the query to your clipboard, or choose **Populate to editor**. If populated to the editor, you can edit the generated query to fit your needs.
6. To save this query to a new query, choose **Save As**.
   - In the **Query Name** field, update the name of the query.
   - In the **Description** field, update the description of the query.
   - Enter up to 50 unique tags for this query.
   - Choose **Save**.
7. Choose **Run**. The query results display in the table below the query editor.
8. Choose **Export as** to export the query results in CSV or JSON format.

> **Note**
>
> The query results are paginated. When you export, up to 500 results are exported. You can also use the APIs to retrieve all the results. The results are paginated and you can retrieve 100 results at a time.

## Example prompts

The following are prompts and the generate queries which you can use as examples.

Example: What load balancers were created after January 1, 2024?

**Prompt**: What load balancers were created after January 1, 2024?

**Generated query**:

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: Which of my RDS database instances are publicly accessible?

**Prompt**: Which of my RDS database instances are publicly accessible?

**Generated query**:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: How many EC2 instances were created in last one year?

**Prompt**: How many EC2 instances were created in last one year?

**Generated query**:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
```

```
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: How many EC2 instances do I have in each of my AWS accounts?

**Prompt**: How many EC2 instances do I have in each of my AWS accounts?

**Generated query**:

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: Which IAM roles have the managed policy AdministratorAccess attached?

**Prompt**: Which IAM roles have the managed policy AdministratorAccess attached?

**Generated query**:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: EBS volumes without encryption

**Prompt**: EBS volumes without encryption

**Generated query**:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
```

```
    configuration.encrypted = false
```

Example: Get noncompliant resources

**Prompt**: Get noncompliant resources

**Generated query**:

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: List all my lambda function that is running node js 16

**Prompt**: List all my lambda function that is running node js 16

**Generated query**:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: What ACM certificates expire the next 30 days?

**Prompt**: What ACM certificates expire the next 30 days?

**Generated query**:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
```

```
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> The times in the generated query depend on the time when you enter the prompt.

## Providing feedback

You can provide overall feedback about the natural language query processor or feedback about a specific generated query.

### Providing feedback on the natural language query processor

Choose the **Provide feedback** button that appears above natural language query processor to the right. You can enter your satisfaction or dissatisfaction and provide feedback on how AWS Config can make the natural language query more helpful.

> **Note**
>
> Do not disclose any personal, commercially sensitive, or confidential information.

### Providing feedback on a specific generated query

You can provide your feedback on a generated query by choose the thumbs up or thumbs down button that appears below the generated query.

## Region Support

The natural language query processor is supported in the following Regions.

| Region Name | Region | Endpoint | Protocol |
| --- | --- | --- | --- |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
| --- | --- | --- | --- |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |

# Example Queries for AWS Config

View the following example queries.

Query to list all EC2 instances with AMI ID ami-12345

Query:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Results:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
```

```
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

## Query for count of resources grouped by their AWS Config rules compliance status

Query:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
```

```
GROUP BY
    configuration.complianceType
```

Results:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

## Query for the compliance status of AWS Conformance packs

Query:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Results:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
```

```
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

## Query to get counts of AWS resources grouped by account ID

Query:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Results:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
```

```
            {
                "Name": "accountId"
            }
        ]
    }
}
```

## Query to list all EC2 volumes that are not in use

### Query:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

### Results:

```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
```

```
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
```

```
}
```

# Example Relationship Queries for AWS Config

View the following example relationship queries.

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

OR

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
```

```
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

# Limitations

**Note**

Advanced query does not support querying resources which have not been configured to be recorded by the configuration recorder. AWS Config creates Configuration Items (CIs) with `ResourceNotRecorded` in the `configurationItemStatus` when a resource has been discovered but is not configured to be recorded by the configuration recorder. While

an aggregator will aggregate these CIs, advanced query does not support querying CIs with `ResourceNotRecorded`. Update your recorder settings to enable recording of the resource types that you want to query.

As a subset of SQL `SELECT`, the query syntax has following limitations:

- No support for `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN`, and `UNION` keywords in a query. `NULL` value queries are not supported.
- No support for complex `CASE` statements for creating a priority field directly in the query.
- No support for querying on third-party resources. Third-party resources retrieved using advanced queries will have the configuration field set as `NULL`.
- No support for nested structures (such as tags) to be unpacked with SQL queries.
- No support for querying deleted resources. To discover deleted resources, see Looking Up Resources That Are Discovered by AWS Config.
- The `SELECT` all columns shorthand (that is `SELECT *`) selects only the top-level, scalar properties of a CI. The scalar properties returned are `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType`, and `version`.
- Wildcard limitations:
  - Wildcards are supported only for property values and not for property keys (for example, `...WHERE someKey LIKE 'someValue%'` is supported but `...WHERE 'someKey%' LIKE 'someValue%'` is not supported).
  - Support for only suffix wildcards (for example, `...LIKE 'AWS::EC2::%'` and `...LIKE 'AWS::EC2::_'` is supported but `...LIKE '%::EC2::Instance'` and `...LIKE '_::EC2::Instance'`is not supported).
  - Wildcard matches must be at least three characters long (for example, `...LIKE 'ab%'` and `...LIKE 'ab_'` is not allowed but `...LIKE 'abc%'` and `...LIKE 'abc_'` is allowed).

  **Note**

  The "_" (single underscore) is also treated as a wildcard.

- Aggregation limitations:
  - Aggregate functions can accept only a single argument or property.

- Aggregate functions cannot take other functions as arguments.
- `GROUP BY` with an `ORDER BY` clause referencing aggregate functions may contain only a single property.
- For all other aggregations `GROUP BY` clauses may contain up to three properties.
- Pagination is supported for all aggregate queries except when `ORDER BY` clause has an aggregate function. For example, `GROUP BY X, ORDER BY Y` does not work if `Y` is an aggregate function.
- No support for `HAVING` clauses in aggregations.

- Mismatched identifier limitations:

  Mismatched identifiers are properties that have the same spelling but different cases (upper and lower case). Advanced query does not support processing queries that contain mismatched identifiers. For example:

  - Two properties that have the exact same spelling but with different casing (`configuration.dbclusterIdentifier` and `configuration.dBClusterIdentifier`).
  - Two properties where one property is a subset of the other, and they have different casing (`configuration.ipAddress` and `configuration.ipaddressPermissions`).

## CIDR notation/IP range behavior for advanced queries

CIDR notation is converted to IP ranges for search.

This means that `"="` and `"BETWEEN"` search for any range that includes the provided IP, instead of for an exact one.

To search for an exact IP range, you need to add in additional conditions to exclude IPs outside of the range.

**Example Searching for exact CIDR block 10.0.0.0/24**

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

**Example Searching for exact IP address 192.168.0.2/32**

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

# Multiple properties within an array behavior for advanced queries

When querying against multiple properties within an array of objects, matches are computed against *all the array elements*.

For example, for a resource R with rules A and B, the resource is compliant to rule A but noncompliant to rule B. The resource R is stored as:

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R will be returned by this query:

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

The first condition `configuration.configRuleList.complianceType = 'non_compliant'` is applied to ALL elements in R.configRuleList, because R has a rule (rule B) with complianceType = 'non_compliant', the condition is evaluated as true.

The second condition `configuration.configRuleList.configRuleName` is applied to ALL elements in R.configRuleList, because R has a rule (rule A) with configRuleName = 'A', the condition is evaluated as true. As both conditions are true, R will be returned.

## Region Support

Advanced queries is supported in the following Regions:

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| US East (Ohio) | us-east-2 | config.us-east-2.amazonaws.com | HTTPS |
| US East (N. Virginia) | us-east-1 | config.us-east-1.amazonaws.com | HTTPS |
| US West (N. California) | us-west-1 | config.us-west-1.amazonaws.com | HTTPS |
| US West (Oregon) | us-west-2 | config.us-west-2.amazonaws.com | HTTPS |
| Africa (Cape Town) | af-south-1 | config.af-south-1.amazonaws.com | HTTPS |
| Asia Pacific (Hong Kong) | ap-east-1 | config.ap-east-1.amazonaws.com | HTTPS |
| Asia Pacific | ap-south-2 | config.ap-south-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| (Hyderabad) | | | |
| Asia Pacific (Jakarta) | ap-southeast-3 | config.ap-southeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Malaysia) | ap-southeast-5 | config.ap-southeast-5.amazonaws.com | HTTPS |
| Asia Pacific (Melbourne) | ap-southeast-4 | config.ap-southeast-4.amazonaws.com | HTTPS |
| Asia Pacific (Mumbai) | ap-south-1 | config.ap-south-1.amazonaws.com | HTTPS |
| Asia Pacific (New Zealand) | ap-southeast-6 | config.ap-southeast-6.amazonaws.com | HTTPS |
| Asia Pacific (Osaka) | ap-northeast-3 | config.ap-northeast-3.amazonaws.com | HTTPS |
| Asia Pacific (Seoul) | ap-northeast-2 | config.ap-northeast-2.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| Asia Pacific (Singapore) | ap-southeast-1 | config.ap-southeast-1.amazonaws.com | HTTPS | |
| Asia Pacific (Sydney) | ap-southeast-2 | config.ap-southeast-2.amazonaws.com | HTTPS | |
| Asia Pacific (Taipei) | ap-east-2 | config.ap-east-2.amazonaws.com | HTTPS | |
| Asia Pacific (Thailand) | ap-southeast-7 | config.ap-southeast-7.amazonaws.com | HTTPS | |
| Asia Pacific (Tokyo) | ap-northeast-1 | config.ap-northeast-1.amazonaws.com | HTTPS | |
| Canada (Central) | ca-central-1 | config.ca-central-1.amazonaws.com | HTTPS | |
| Canada West (Calgary) | ca-west-1 | config.ca-west-1.amazonaws.com | HTTPS | |
| Europe (Frankfurt) | eu-central-1 | config.eu-central-1.amazonaws.com | HTTPS | |
| Europe (Ireland) | eu-west-1 | config.eu-west-1.amazonaws.com | HTTPS | |

| Region Name | Region | Endpoint | Protocol |
|---|---|---|---|
| Europe (London) | eu-west-2 | config.eu-west-2.amazonaws.com | HTTPS |
| Europe (Milan) | eu-south-1 | config.eu-south-1.amazonaws.com | HTTPS |
| Europe (Paris) | eu-west-3 | config.eu-west-3.amazonaws.com | HTTPS |
| Europe (Spain) | eu-south-2 | config.eu-south-2.amazonaws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | config.eu-north-1.amazonaws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | config.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | config.il-central-1.amazonaws.com | HTTPS |
| Mexico (Central) | mx-central-1 | config.mx-central-1.amazonaws.com | HTTPS |
| Middle East (Bahrain) | me-south-1 | config.me-south-1.amazonaws.com | HTTPS |
| Middle East (UAE) | me-central-1 | config.me-central-1.amazonaws.com | HTTPS |

| Region Name | Region | Endpoint | Protocol | |
|---|---|---|---|---|
| South America (São Paulo) | sa-east-1 | config.sa-east-1.amazonaws.com | HTTPS | |
| AWS GovCloud (US-East) | us-gov-east-1 | config.us-gov-east-1.amazonaws.com | HTTPS | |
| AWS GovCloud (US-West) | us-gov-west-1 | config.us-gov-west-1.amazonaws.com | HTTPS | |

# Deleting AWS Config Data

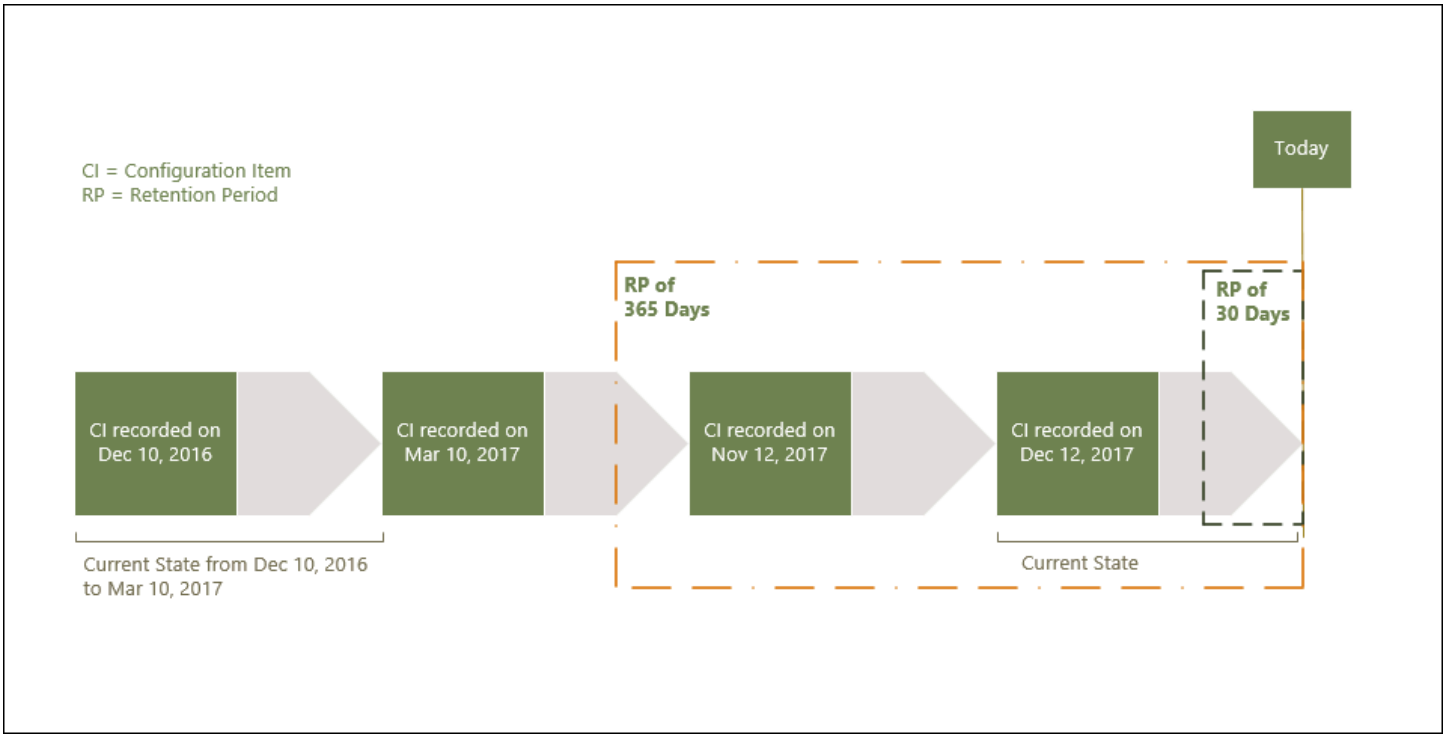
> **Note**
>
> While AWS Config uses Amazon Simple Storage Service (Amazon S3) and Amazon Simple Notification Service (Amazon SNS) for sending configuration snapshots and configuration history files, AWS Config has its own data store and retention policies. The information on this page is specific for AWS Config. Amazon S3 and Amazon SNS have their own separate data store and retention policies.

AWS Config allows you to delete your data by specifying a retention period for your `ConfigurationItems`. When you specify a retention period, AWS Config retains your `ConfigurationItems` for that specified period. You can choose a period between a minimum of 30 days and a maximum of 7 years (2557 days). AWS Config deletes data older than your specified retention period. If you do not specify a retention period, AWS Config continues to store `ConfigurationItems` for the default period of 7 years (2557 days). When recording is switched on, the current state of the resource is when a `ConfigurationItem` is recorded and until the next change (a new `ConfigurationItem`) is recorded.

To understand the behavior of retention period, let's take a look at the timeline.

- When recording is switched on, the current state of a resource always exists and can't be deleted irrespective of the date the `ConfigurationItem` is recorded.
- When AWS Config records new `ConfigurationItems`, the previous `ConfigurationItems` are deleted depending on the specified retention period.

In the following timeline, AWS Config records `ConfigurationItems` at the following dates. For the purpose of this timeline, today is represented as May 24, 2018.




The following table explains which `ConfigurationItems` are displayed on the AWS Config timeline based on selected retention period.

| Retention Period | Configuration Items displayed on timeline | Explanation |
| --- | --- | --- |
| 30 days | December 12, 2017 | The current state of the resource started from December 12, 2017 when the `ConfigurationItem` was recorded and is valid until today (May 24, 2018). When recording is turned on, the current state always exists. |
| 365 days | December 12, 2017; November 12, 2017, and March 10, 2017 | The retention period shows the current state December 12, 2017 and previous `ConfigurationItems` November 12, 2017 and March 10, 2017. |

| Retention Period | Configuration Items displayed on timeline | Explanation |
| --- | --- | --- |
| | | The `ConfigurationItem` for March 10, 2017 is displayed on the timeline because that configuration state represented the current state 365 days ago. |

After you specify a retention period, AWS Config APIs no longer return `ConfigurationItems` that represent a state older than the specified retention period.

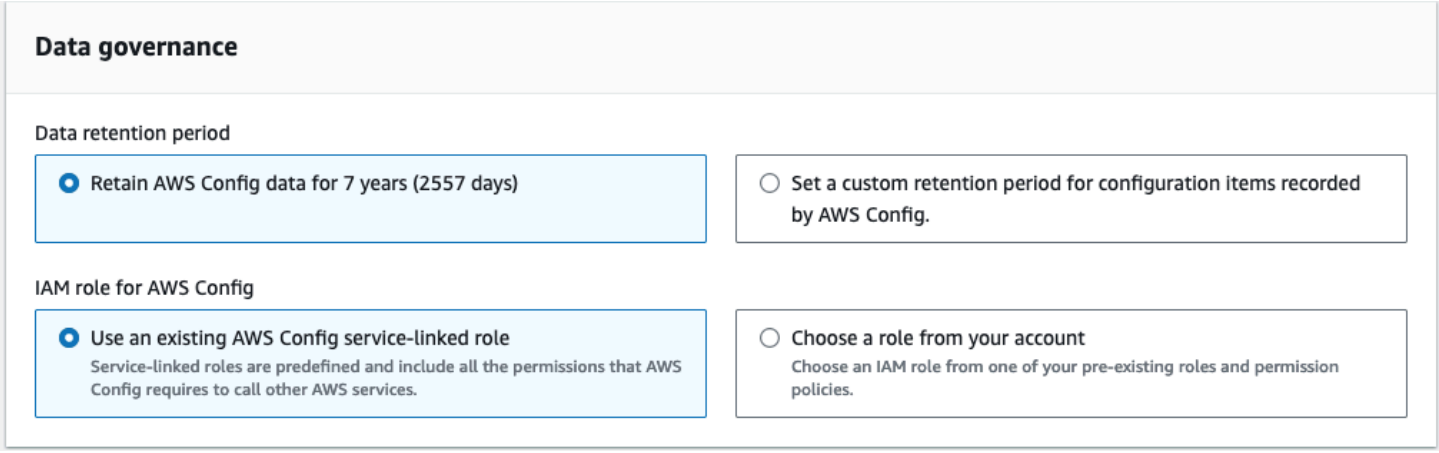
> **Note**
>
> - AWS Config cannot record your `ConfigurationItems` if recording is switched off.
> - AWS Config cannot record your `ConfigurationItems` if your IAM role has insufficient permissions. For more information, see Permissions for the IAM Role Assigned to AWS Config.

## Setting Data Retention Period in AWS Management Console

In the AWS Management Console, if you do not select a data retention period, the default period is 7 years or 2557 days.

To set a custom data retention period for configuration items select the checkbox. You can select 1 year, 3 years, 5 years, or a custom period. For a custom period, enter the number of days between 30 and 2557 days.

The following image displays where you can set the data retention period in **Data Governance**. You can access **Data Governance** on the **Edit Settings** page from the AWS Config console by choosing **Settings** in the left navigation bar, and then choosing **Edit**.


Data governance
Data retention period
Retain AWS Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by AWS Config.
IAM role for AWS Config
Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

# Security in AWS Config

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Config, see AWS services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using AWS Config. The following topics show you how to configure AWS Config to meet your security and compliance objectives.

**Topics**


- Data Protection in AWS Config
- Identity and Access Management for AWS Config
- Incident Response in AWS Config
- Compliance Validation for AWS Config
- Resilience in AWS Config
- Infrastructure Security in AWS Config
- Cross-service confused deputy prevention
- Security Best Practices for AWS Config

# Data Protection in AWS Config

The AWS shared responsibility model applies to data protection in AWS Config. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with AWS Config or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

## Encryption of Data at Rest

Data is encrypted at rest using transparent server-side encryption. This helps reduce the operational burden and complexity involved in protecting sensitive data. With encryption at rest, you can build security-sensitive applications that meet encryption compliance and regulatory requirements.

## Encryption of Data in Transit

Data gathered and accessed by AWS Config is exclusively over a Transport Layer Security (TLS) protected channel.

# Identity and Access Management for AWS Config

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use AWS Config resources. IAM is an AWS service that you can use with no additional charge.

**Topics**


- Audience
- Authenticating with identities
- Managing access using policies
- How AWS Config works with IAM
- Identity-based policy examples for AWS Config
- AWS managed policies for AWS Config
- Permissions for the IAM Role Assigned to AWS Config
- Updating the IAM Role for the customer managed configuration recorder
- Permissions for the Amazon S3 Bucket for the AWS Config Delivery Channel
- Permissions for the KMS Key for the AWS Config Delivery Channel
- Permissions for the Amazon SNS Topic
- Troubleshooting AWS Config identity and access
- Using Service-Linked Roles for AWS Config

## Audience

How you use AWS Identity and Access Management (IAM) differs based on your role:

- **Service user** - request permissions from your administrator if you cannot access features (see Troubleshooting AWS Config identity and access)
- **Service administrator** - determine user access and submit permission requests (see How AWS Config works with IAM)
- **IAM administrator** - write policies to manage access (see Identity-based policy examples for AWS Config)

## Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

### AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see Tasks that require root user credentials in the *IAM User Guide*.

### Federated identity

As a best practice, require human users to use federation with an identity provider to access AWS services using temporary credentials.

A *federated identity* is a user from your enterprise directory, web identity provider, or Directory Service that accesses AWS services using credentials from an identity source. Federated identities assume roles that provide temporary credentials.

For centralized access management, we recommend AWS IAM Identity Center. For more information, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

### IAM users and groups

An *IAM user* is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more information, see Require human users to use federation with an identity provider to access AWS using temporary credentials in the *IAM User Guide*.

An *IAM group* specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see Use cases for IAM users in the *IAM User Guide*.

### IAM roles

An *IAM role* is an identity with specific permissions that provides temporary credentials. You can assume a role by switching from a user to an IAM role (console) or by calling an AWS CLI or AWS API operation. For more information, see Methods to assume a role in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

## Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

## Identity-based policies

Identity-based policies are JSON permissions policy documents that you attach to an identity (user, group, or role). These policies control what actions identities can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between managed and inline policies, see Choose between managed policies and inline policies in the *IAM User Guide*.

## Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples include IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. You must specify a principal in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

## Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. For more information, see Session policies in the *IAM User Guide*.

### Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

## How AWS Config works with IAM

Before you use IAM to manage access to AWS Config, learn what IAM features are available to use with AWS Config.

**IAM features you can use with AWS Config**

| IAM feature | AWS Config support |
| --- | --- |
| Identity-based policies | Yes |
| Resource-based policies | No |
| Policy actions | Yes |
| Policy resources | Yes |
| Policy condition keys (service-specific) | Yes |
| ACLs | No |
| ABAC (tags in policies) | Yes |
| Temporary credentials | Yes |
| Forward access sessions (FAS) | Yes |
| Service roles | Yes |
| Service-linked roles | Yes |

To get a high-level view of how AWS Config and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

## Identity-based policies for AWS Config

**Supports identity-based policies:** Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

### Identity-based policy examples for AWS Config

To view examples of AWS Config identity-based policies, see Identity-based policy examples for AWS Config.

## Resource-based policies within AWS Config

**Supports resource-based policies:** No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

## Policy actions for AWS Config

**Supports policy actions:** Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Include actions in a policy to grant permissions to perform the associated operation.

To see a list of AWS Config actions, see Actions defined by AWS Config in the *Service Authorization Reference*.

Policy actions in AWS Config use the following prefix before the action:

```
config
```

To specify multiple actions in a single statement, separate them with commas.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "config:Describe*"
```

To view examples of AWS Config identity-based policies, see Identity-based policy examples for AWS Config.

## Policy resources for AWS Config

**Supports policy resources:** Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't support resource-level permissions, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

To see a list of AWS Config resource types and their ARNs, see Resources defined by AWS Config in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions defined by AWS Config.

To view examples of AWS Config identity-based policies, see Identity-based policy examples for AWS Config.

## Policy condition keys for AWS Config

**Supports service-specific policy condition keys:** Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of AWS Config condition keys, see Condition keys for AWS Config in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions defined by AWS Config.

To view examples of AWS Config identity-based policies, see Identity-based policy examples for AWS Config.

## ACLs in AWS Config

**Supports ACLs:** No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

## ABAC with AWS Config

**Supports ABAC (tags in policies):** Yes

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes called tags. You can attach tags to IAM entities and AWS resources, then design ABAC policies to allow operations when the principal's tag matches the tag on the resource.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

For more information about tagging AWS Config resources, see Tagging Your AWS Config Resources.

## Using temporary credentials with AWS Config

**Supports temporary credentials:** Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

## Forward access sessions for AWS Config

**Supports forward access sessions (FAS):** Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

## Service roles for AWS Config

**Supports service roles:** Yes

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break AWS Config functionality. Edit service roles only when AWS Config provides guidance to do so.

### Service-linked roles for AWS Config

**Supports service-linked roles:** Yes

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing AWS Config service-linked roles, see Using Service-Linked Roles for AWS Config.

For details about creating or managing service-linked roles, see AWS services that work with IAM. Find a service in the table that includes a `Yes` in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

## Identity-based policy examples for AWS Config

By default, users and roles don't have permission to create or modify AWS Config resources. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Create IAM policies (console) in the *IAM User Guide*.

For details about actions and resource types defined by AWS Config, including the format of the ARNs for each of the resource types, see Actions, resources, and condition keys for AWS Config in the *Service Authorization Reference*.

**Topics**


- Policy best practices
- Sign up for an AWS account
- Create a user with administrative access

- Using the AWS Config console
- Allow users to view their own permissions
- Read-only access to AWS Config
- Full access to AWS Config
- Supported Resource-Level Permissions for AWS Config Rule API Actions
- Supported Resource-Level Permissions for Multi-Account Multi-Region Data Aggregation

## Policy best practices

Identity-based policies determine whether someone can create, access, or delete AWS Config resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see Validate policies with IAM Access Analyzer in the *IAM User Guide*.

- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Secure API access with MFA in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

## Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

**To sign up for an AWS account**

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call or text message and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

## Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

**Secure your AWS account root user**

1. Sign in to the AWS Management Console as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

For help signing in by using root user, see Signing in as the root user in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the *IAM User Guide*.

**Create a user with administrative access**

1. Enable IAM Identity Center.

   For instructions, see Enabling AWS IAM Identity Center in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see Configure user access with the default IAM Identity Center directory in the *AWS IAM Identity Center User Guide*.

**Sign in as the user with administrative access**

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the *AWS Sign-In User Guide*.

**Assign access to additional users**

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

   For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

   For instructions, see Add groups in the *AWS IAM Identity Center User Guide*.

## Using the AWS Config console

To access the AWS Config console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the AWS Config resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the AWS Config console, also attach the AWS Config `AWSConfigUserAccess` AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

You must give users permissions to interact with AWS Config. For users who need full access to AWS Config, use the Full access to AWS Config managed policy.

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

  Create a permission set. Follow the instructions in Create a permission set in the *AWS IAM Identity Center User Guide*.
- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Create a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Create a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

## Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Read-only access to AWS Config

The following example shows an AWS managed policy, `AWSConfigUserAccess` that grants read-only access to AWS Config.

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

In the policy statements, the `Effect` element specifies whether the actions are allowed or denied. The `Action` element lists the specific actions that the user is allowed to perform. The `Resource` element lists the AWS resources the user is allowed to perform those actions on. For policies that control access to AWS Config actions, the `Resource` element is always set to `*`, a wildcard that means "all resources."

The values in the `Action` element correspond to the APIs that the services support. The actions are preceded by `config:` to indicate that they refer to AWS Config actions. You can use the `*` wildcard character in the `Action` element, such as in the following examples:

- `"Action": ["config:*ConfigurationRecorder"]`

  This allows all AWS Config actions that end with "ConfigurationRecorder" (`StartConfigurationRecorder`, `StopConfigurationRecorder`).

- `"Action": ["config:*"]`

  This allows all AWS Config actions, but not actions for other AWS services.

- `"Action": ["*"]`

This allows all AWS actions. This permission is suitable for a user who acts as an AWS administrator for your account.

The read-only policy doesn't grant user permission for the actions such as `StartConfigurationRecorder`, `StopConfigurationRecorder`, and `DeleteConfigurationRecorder`. Users with this policy are not allowed to start configuration recorder, stop configuration recorder, or delete configuration recorder. For the list of AWS Config actions, see the AWS Config API Reference.

## Full access to AWS Config

The following example shows a policy that grants full access to AWS Config. It grants users the permission to perform all AWS Config actions. It also lets users manage files in Amazon S3 buckets and manage Amazon SNS topics in the account that the user is associated with.

> **Important**
>
> This policy grants broad permissions. Before granting full access, consider starting with a minimum set of permissions and granting additional permissions as necessary. Doing so is better practice than starting with permissions that are too lenient and then trying to tighten them later.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

## Supported Resource-Level Permissions for AWS Config Rule API Actions

Resource-level permissions refers to the ability to specify which resources users are allowed to perform actions on. AWS Config supports resource-level permissions for certain AWS Config rule API actions. This means that for certain AWS Config rule actions, you can control the conditions under which when users are allowed to use those actions. These conditions can be actions that must be fulfilled, or specific resources that users are allowed to use.

The following table describes the AWS Config rule API actions that currently support resource-level permissions. It also describes the supported resources and their ARNs for each action. When specifying an ARN, you can use the * wildcard in your paths; for example, when you cannot or do not want to specify exact resource IDs.

> **Important**
>
> If an AWS Config rule API action is not listed in this table, then it does not support resource-level permissions. If an AWS Config rule action does not support resource-level permissions, you can grant users permissions to use the action, but you have to specify a * for the resource element of your policy statement.

| API Action | Resources |
| --- | --- |
| DeleteConfigRule | Config Rule<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| DeleteEvaluationResults | Config Rule<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| DescribeCompliance ByConfigRule | Config Rule<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |

| API Action | Resources |
| --- | --- |
| DescribeConfigRuleEvaluationStatus | Config Rule<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| GetComplianceDetailsByConfigRule | Config Rule<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| PutConfigRule | Config Rule<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| StartConfigRulesEvaluation | Config Rule<br><br>arn:aws:config:*region:accountID* :config-rule/config-rule-*ID* |
| PutRemediationConfigurations | Remediation Configuration<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id* |
| DescribeRemediationConfigurations | Remediation Configuration<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id* |
| DeleteRemediationConfiguration | Remediation Configuration<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id* |

| API Action | Resources |
| --- | --- |
| PutRemediationExceptions | Remediation Configuration<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id* |
| DescribeRemediationExceptions | Remediation Configuration<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id* |
| DeleteRemediationExceptions | Remediation Configuration<br><br>arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id* |

For example, you want to allow read access and deny write access to specific rules to specific users.

In the first policy, you allow the AWS Config rule read actions such as `DescribeConfigRuleEvaluationStatus` on the specified rules.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "config:StartConfigRulesEvaluation",
                "config:DescribeComplianceByConfigRule",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": [
```

```
                "arn:aws:config:us-east-1:123456789012:config-rule/config-
rule-ID",
                "arn:aws:config:us-east-1:123456789012:config-rule/config-
rule-ID"
            ]
        }
    ]
}
```

In the second policy, you deny the AWS Config rule write actions on the specific rule.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
            ],
            "Resource": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-ID"
        }
    ]
}
```

With resource-level permissions, you can allow read access and deny write access to perform specific actions on AWS Config rule API actions.

## Supported Resource-Level Permissions for Multi-Account Multi-Region Data Aggregation

You can use resource-level permissions to control a user's ability to perform specific actions on multi-account multi-region data aggregation. The following AWS Config `Aggregator` APIs support resource level permissions:

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

For example, you can restrict access to resource data from specific users by creating two aggregators `AccessibleAggregator` and `InAccessibleAggregator` and attaching an IAM policy that allows access to `AccessibleAggregator` but denies access to `InAccessibleAggregator`.

**IAM Policy for AccessibleAggregator**

In this policy, you allow access to the supported aggregator actions for the AWS Config Amazon Resource Name (ARN) that you specify. In this example, the AWS Config ARN is `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
```

```
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-mocpsqhs"
        }
    ]
}
```

### IAM Policy for InAccessibleAggregator

In this policy, you deny access to the supported aggregator actions for the AWS Config ARN that you specify. In this example, the AWS Config ARN is `arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
```

```
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

If a user of the developer group tries to perform any of these actions on the AWS Config ARN that you specified, that user will get an access denied exception.

### Checking User Access Permissions

To show the aggregators that you have created, run the following AWS CLI command:

```
aws configservice describe-configuration-aggregators
```

When command has successfully completed, you will be able to see the details for all the aggregators associated with your account. In this example, those are `AccessibleAggregator` and `InAccessibleAggregator`:

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
```

```
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

**Note**

For `account-aggregation-sources` enter a comma-separated list of AWS account IDs for which you want to aggregate data. Wrap the account IDs in square brackets, and be sure to escape quotation marks (for example, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).

Attach the following IAM policy to deny access to `InAccessibleAggregator`, or the aggregator to which you want to deny access.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

Next, you can confirm that the IAM policy works for restricting access to rules for a specific aggregator:

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

The command should return an access denied exception:

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

# AWS managed policies for AWS Config

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the *IAM User Guide*.

## AWS managed policy: AWSConfigServiceRolePolicy

AWS Config uses the service-linked role named **AWSServiceRoleForConfig** to call other AWS services on your behalf. When you use the AWS Management Console to set up AWS Config, this SLR is automatically created by AWS Config if you select the option to use the AWS Config SLR instead of your own AWS Identity and Access Management (IAM) service role.

The **AWSServiceRoleForConfig** SLR contains the managed policy `AWSConfigServiceRolePolicy`. This managed policy contains read-only and write-only permissions for AWS Config resources and read-only permissions for resources in other services that AWS Config supports. The policy provides comprehensive access to monitor and record configuration changes across your AWS infrastructure, including permissions for over 100 AWS services such as compute, storage, networking, security, analytics, and machine learning services.

The policy includes permissions for the following service categories:

- `access-analyzer` – Allows principals to analyze access patterns and retrieve security findings.
- `account` – Allows principals to retrieve account contact information.
- `acm` and `acm-pca` – Allows principals to manage SSL/TLS certificates and private certificate authorities.

- `airflow` – Allows principals to monitor managed Apache Airflow environments.
- `amplify` and `amplifyuibuilder` – Allows principals to monitor web applications and UI components.
- `aoss` – Allows principals to monitor OpenSearch Serverless collections and security configurations.
- `app-integrations` – Allows principals to monitor application integration configurations.
- `appconfig` – Allows principals to monitor application configuration deployments.
- `appflow` – Allows principals to monitor data flow configurations between applications.
- `application-autoscaling` and `application-signals` – Allows principals to monitor auto-scaling policies and application performance metrics.
- `appmesh` – Allows principals to monitor service mesh configurations.
- `apprunner` – Allows principals to monitor containerized web applications and services.
- `appstream` – Allows principals to monitor application streaming configurations.
- `appsync` – Allows principals to monitor GraphQL API configurations.
- `aps` – Allows principals to monitor Prometheus monitoring configurations.
- `apptest` – Allows principals to monitor application testing configurations.
- `arc-zonal-shift` – Allows principals to monitor zonal shift configurations for availability.
- `athena` – Allows principals to monitor query engine configurations and data catalogs.
- `auditmanager` – Allows principals to monitor audit and compliance assessments.
- `autoscaling` and `autoscaling-plans` – Allows principals to monitor auto-scaling groups and scaling plans.
- `b2bi` – Allows principals to monitor business-to-business integration configurations.
- `backup` and `backup-gateway` – Allows principals to monitor backup policies and gateway configurations.
- `batch` – Allows principals to monitor batch computing environments and job queues.
- `bcm-data-exports` – Allows principals to monitor billing and cost management data exports.
- `bedrock` and `bedrock-agentcore` – Allows principals to monitor foundation models and AI agent configurations.
- `billingconductor` – Allows principals to monitor billing group configurations.
- `budgets` – Allows principals to monitor budget configurations and actions.
- `cassandra` – Allows principals to query managed Cassandra database configurations.

- `ce` – Allows principals to monitor cost and usage reporting configurations.
- `cleanrooms` and `cleanrooms-ml` – Allows principals to monitor data collaboration and machine learning configurations.
- `cloud9` – Allows principals to monitor cloud development environment configurations.
- `cloudformation` – Allows principals to monitor infrastructure as code stack configurations.
- `cloudfront` – Allows principals to monitor content delivery network configurations.
- `cloudtrail` – Allows principals to monitor API logging and audit trail configurations.
- `cloudwatch` – Allows principals to monitor metrics, alarms, and dashboard configurations.
- `codeartifact` – Allows principals to monitor software package repository configurations.
- `codebuild` – Allows principals to monitor build project configurations.
- `codecommit` – Allows principals to monitor source code repository configurations.
- `codeconnections` – Allows principals to monitor third-party source connections.
- `codedeploy` – Allows principals to monitor application deployment configurations.
- `codeguru-profiler` and `codeguru-reviewer` – Allows principals to monitor code analysis and profiling configurations.
- `codepipeline` – Allows principals to monitor continuous integration and deployment pipeline configurations.
- `codestar-connections` – Allows principals to monitor developer tool connections.
- `cognito-identity` and `cognito-idp` – Allows principals to monitor identity and user pool configurations.
- `comprehend` – Allows principals to monitor natural language processing configurations.
- `config` – Allows principals to manage configuration recording and compliance monitoring.
- `connect` – Allows principals to monitor contact center configurations.

For more information about supported resource types, see Supported Resource Types for AWS Config and Using Service-Linked Roles for AWS Config.

To view more details about the policy, including the latest version of the JSON policy document, see AWSConfigServiceRolePolicy in the *AWS Managed Policy Reference Guide*.

> **Recommended: Use the Service-linked role**
>
> It is recommended that you use the service-linked role unless you have a particular use case. A service-linked role adds all the necessary permissions for AWS Config to run as expected. Some features such as service-linked configuration recorders require you to use the service-linked role.

## AWS managed policy: AWS_ConfigRole

To record your AWS resource configurations, AWS Config requires IAM permissions to get the configuration details about your resources. If you want to create an IAM role for AWS Config, you can use the managed policy `AWS_ConfigRole` and attach it to your IAM role.

This IAM policy is updated each time AWS Config adds support for an AWS resource type. This means that AWS Config will continue to have the required permissions to record configuration data of supported resource types as long as the **AWS_ConfigRole** role has this managed policy attached. The policy provides comprehensive access to monitor and record configuration changes across your AWS infrastructure, including permissions for over 100 AWS services such as compute, storage, networking, security, analytics, and machine learning services. For more information, see Supported Resource Types for AWS Config and Permissions for the IAM Role Assigned to AWS Config.

To view more details about the policy, including the latest version of the JSON policy document, see AWS_ConfigRole in the *AWS Managed Policy Reference Guide*.

## AWS managed policy: AWSConfigUserAccess

This IAM policy provides access to use AWS Config, including searching by tags on resources and reading all tags. This does not provide permission to configure AWS Config, which requires administrative privileges.

View the policy: AWSConfigUserAccess.

## AWS managed policy: ConfigConformsServiceRolePolicy

To deploy and manage conformance packs, AWS Config requires IAM permissions and certain permissions from other AWS services. These allow you to deploy and manage conformance packs with full functionality and are updated each time AWS Config adds new functionality for conformance packs. For more information on conformance packs, see Conformance packs.

View the policy: ConfigConformsServiceRolePolicy.

## AWS managed policy: AWSConfigRulesExecutionRole

To deploy AWS Custom Lambda Rules, AWS Config requires IAM permissions and certain permissions from other AWS services. These allow AWS Lambda functions to access the AWS Config API and the configuration snapshots that AWS Config delivers periodically to Amazon S3. This access is required by functions that evaluate configuration changes for AWS Custom Lambda rules and is updated each time AWS Config adds new functionality. For more information on AWS Custom Lambda Rules, see Creating AWS Config Custom Lambda Rules. For more information on configuration snapshots, see Concepts | Configuration Snapshot. For more information on the delivery of configuration snapshots, see Managing the Delivery Channel.

View the policy: AWSConfigRulesExecutionRole.

## AWS managed policy: AWSConfigMultiAccountSetupPolicy

To centrally deploy, update, and delete AWS Config rules and conformance packs across member accounts in an organization in AWS Organizations, AWS Config requires IAM permissions and certain permissions from other AWS services. This managed policy is updated each time AWS Config adds new functionality for multi-account setup. For more information, see Managing AWS Config Rules Across All Accounts in Your Organization and Managing Conformance Packs Across All Accounts in Your Organization.

View the policy: AWSConfigMultiAccountSetupPolicy.

## AWS managed policy: AWSConfigRoleForOrganizations

To allow AWS Config to call read-only AWS Organizations APIs, AWS Config requires IAM permissions and certain permissions from other AWS services. This managed policy is updated each time AWS Config adds new functionality for multi-account setup. For more information, see Managing AWS Config Rules Across All Accounts in Your Organization and Managing Conformance Packs Across All Accounts in Your Organization.

View the policy: AWSConfigRoleForOrganizations.

## AWS managed policy: AWSConfigRemediationServiceRolePolicy

To allow AWS Config to remediate `NON_COMPLIANT` resources on your behalf, AWS Config requires IAM permissions and certain permissions from other AWS services. This managed policy is updated each time AWS Config adds new functionality for remediation. For more information

on remediation, see Remediating Noncompliant Resources with AWS Config Rules. For more information on the conditions that initiate the possible AWS Config evaluation results, see Concepts | AWS Config Rules.

View the policy: AWSConfigRemediationServiceRolePolicy.

## AWS Config updates to AWS managed policies

View details about updates to AWS managed policies for AWS Config since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Config Document history page.

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – add "lightsail:GetActiveNames" "lightsail:GetOperations" "s3:GetBucketAbac" | This policy now supports additional permissions for Amazon Lightsail and Amazon Simple Storage Service (Amazon S3). | November 20, 2025 |
| AWSConfigServiceRolePolicy – add "lightsail:GetActiveNames" "lightsail:GetOperations" "s3:GetBucketAbac" | This policy now supports additional permissions for Amazon Lightsail and Amazon Simple Storage Service (Amazon S3). | November 20, 2025 |
| AWSConfigServiceRolePolicy – Updated managed policy with comprehensive permissions for AWS resource configuration recording across over 100 AWS services including compute, storage, networking, security, analytics, and machine learning services. | This policy now provides enhanced documentation of service permissions and supports comprehensive monitoring across all AWS services that AWS Config supports for configuration recording. | November 11, 2025 |
| AWS_ConfigRole – Updated managed policy with comprehensive permissions | This policy now supports additional permissions for comprehensive AWS resource | November 10, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| for AWS resource configura tion recording across multiple services including AWS Identity and Access Management, Amazon Elastic Compute Cloud, Amazon Simple Storage Service, AWS Lambda, Amazon Relational Database Service, and many others. | configuration recording and monitoring across all supported AWS services. | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – add "amplify:GetDomainAssociation" "amplify:ListDomainAssociations" "amplify:ListTagsForResource" "appsync:GetSourceApiAssociation" "appsync:ListSourceApiAssociations" "bedrock:GetFlow" "bedrock:ListAgentCollaborators" "bedrock:ListFlows" "bedrock:ListPrompts" "cloudTrail:GetResourcePolicy" "cloudformation:DescribePublisher" "codeartifact:DescribePackageGroup" "codeartifact:ListAllowedRepositoriesForGroup" "codeartifact:ListPackageGroups" "codepipeline:ListActionTypes" "codepipeline:ListTagsForResource" "codepipeline:ListWebhooks" "connect:DescribeTrafficDistributionGroup" "connect:ListTrafficDistributionGroups" "deadline:ListFarms" "ec2:GetTransitGatewayRouteTablePropagations" "ec2:SearchLocalGatewayRoutes" "ec2:SearchTransitGatewayMulticastGroups" "entityresolution:GetMatchingWorkflow" "entityresolution:ListMatchingWorkflows" "iotsitewise:ListAssetModelCo | This policy now supports additional permissions for AWS Amplify, AWS AppSync, Amazon Bedrock, AWS CloudTrail, CloudFormation, AWS CodeArtifact, AWS CodePipeline, Amazon Connect, AWS Deadline Cloud, Amazon EC2, AWS Entity Resolution, AWS IoT SiteWise, Amazon IVS, AWS Lambda, Amazon EventBridge, Amazon Quick Suite, Amazon Redshift, Amazon Redshift Serverless, AWS Identity and Access Management Roles Anywhere, Amazon SageMaker, AWS Secrets Manager, Amazon Security Lake, AWS Service Catalog, AWS Shield, Amazon EC2 Systems Manager, and AWS WAFV2. | October 1, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| mpositeModels" "iotsitewise: ListAssetModelProperties" "i otsitewise:ListAssetPropert ies" "iotsitewise:ListA ssociatedAssets" "ivs:ListPu blicKeys" "lambda:GetProvisi onedConcurrencyConfig" "lambda:GetRuntimeManag ementConfig" "lambd a:ListFunctionEventInvokeCo nfigs" "lambda:ListFunctionU rlConfigs" "pipes:DescribePip e" "pipes:ListPipes" "quicksig ht:DescribeRefreshSchedule" "quicksight:ListRefreshSche dules" "redshift-serverless: ListSnapshotCopyConfigurati ons" "redshift:GetResourcePo licy" "rolesanywhere:GetCrl" "rolesanywhere:ListCrls" "sagemaker:DescribeApp" "sagemaker:DescribeUse rProfile" "sagemaker:ListApp s" "sagemaker:ListM odelPackages" "sagemake r:ListUserProfiles" "secrets manager:GetResourcePolicy" "securitylake:ListSubscribe rs" "securitylake:ListTagsFo rResource" "servicecatalog:D escribeServiceAction" "servicecatalog:ListAppl ications" "servicecatalog:Li stAssociatedResources" "shield:ListProtectionG | | |

| Change | Description | Date |
| --- | --- | --- |
| roups" "shield:ListTagsFo rResource" "ssm-incidents:Ge tReplicationSet" "ssm-incide nts:ListReplicationSets" "ssm:DescribeAssociation" "s sm:DescribePatchBaselines" "ssm:GetDefaultPatchBaselin e" "ssm:GetPatchBaseline" "ssm:GetResourcePolicies" "ssm:ListAssociations" "ssm:ListResourceDataSync" " wafv2:ListLoggingConfigurat ions" "bedrock-agentcore:Lis tCodeInterpreters" "bedrock-agentcore:GetCodeInterprete r" "bedrock-agentcore:ListBr owsers" "bedrock-agentcore :GetBrowser" "bedrock-agentcore:ListAgentRunti mes" "bedrock-agent core:GetAgentRuntime" "bedrock-agentcore:ListA gentRuntimeEndpoints" "bedrock-agentcore:GetAg entRuntimeEndpoint" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – add "amplify:GetDomainAssociation" "amplify:ListDomainAssociations" "amplify:ListTagsForResource" "appsync:GetSourceApiAssociation" "appsync:ListSourceApiAssociations" "bedrock:GetFlow" "bedrock:ListAgentCollaborators" "bedrock:ListFlows" "bedrock:ListPrompts" "cloudTrail:GetResourcePolicy" "cloudformation:DescribePublisher" "codeartifact:DescribePackageGroup" "codeartifact:ListAllowedRepositoriesForGroup" "codeartifact:ListPackageGroups" "codepipeline:ListActionTypes" "codepipeline:ListTagsForResource" "codepipeline:ListWebhooks" "connect:DescribeTrafficDistributionGroup" "connect:ListTrafficDistributionGroups" "deadline:ListFarms" "ec2:GetTransitGatewayRouteTablePropagations" "ec2:SearchLocalGatewayRoutes" "ec2:SearchTransitGatewayMulticastGroups" "entityresolution:GetMatchingWorkflow" "entityresolution:ListMatchingWorkflows" "iotsitew | This policy now supports additional permissions for AWS Amplify, AWS AppSync, Amazon Bedrock, AWS CloudTrail, CloudFormation, AWS CodeArtifact, AWS CodePipeline, Amazon Connect, AWS Deadline Cloud, Amazon EC2, AWS Entity Resolution, AWS IoT SiteWise, Amazon IVS, AWS Lambda, Amazon EventBridge, Amazon Quick Suite, Amazon Redshift, Amazon Redshift Serverless, AWS Identity and Access Management Roles Anywhere, Amazon SageMaker, AWS Secrets Manager, Amazon Security Lake, AWS Service Catalog, AWS Shield, Amazon EC2 Systems Manager, and AWS WAFV2. | October 1, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| ise:ListAssetModelComposite Models" "iotsitewise:ListA ssetModelProperties" "iotsitewise:ListAssetProper ties" "iotsitewise:ListA ssociatedAssets" "ivs:List PublicKeys" "lambda:G etProvisionedConcurrencyCon fig" "lambda:GetRuntime ManagementConfig" "lambda:ListFunctionEventIn vokeConfigs" "lambda:L istFunctionUrlConfigs" "pipes:DescribePipe" "pipes:Li stPipes" "quicksight:Descri beRefreshSchedule" "quicksig ht:ListRefreshSchedules" "redshift-serverless:ListSn apshotCopyConfigurations" "redshift:GetResourcePolicy " "rolesanywhere:GetCrl" "rolesanywhere:ListCrls" "sagemaker:DescribeApp" "sagemaker:DescribeUserProf ile" "sagemaker:ListApps" "sagemaker:ListModelPackage s" "sagemaker:ListUse rProfiles" "secretsmanager:Ge tResourcePolicy" "security lake:ListSubscribers" "security lake:ListTagsForResource" "servicecatalog:DescribeSer viceAction" "servicecatalog:Li stApplications" "servicec atalog:ListAssociatedResour | | |

| Change | Description | Date |
| --- | --- | --- |
| ces" "shield:ListProtectionGroups" "shield:ListTagsForResource" "ssm-incidents:GetReplicationSet" "ssm-incidents:ListReplicationSets" "ssm:DescribeAssociation" "ssm:DescribePatchBaselines" "ssm:GetDefaultPatchBaseline" "ssm:GetPatchBaseline" "ssm:GetResourcePolicies" "ssm:ListAssociations" "ssm:ListResourceDataSync" "wafv2:ListLoggingConfigurations" "bedrock-agentcore:ListCodeInterpreters" "bedrock-agentcore:GetCodeInterpreter" "bedrock-agentcore:ListBrowsers" "bedrock-agentcore:GetBrowser" "bedrock-agentcore:ListAgentRuntimes" "bedrock-agentcore:GetAgentRuntime" "bedrock-agentcore:ListAgentRuntimeEndpoints" "bedrock-agentcore:GetAgentRuntimeEndpoint" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "arc-zonal-shift:GetAutoshiftObserverNotificationStatus", "bedrock:GetModelInvocationLoggingConfiguration", "cloudtrail:GetEventConfiguration", "codeartifact:DescribeDomain", "codeartifact:GetDomainPermissionsPolicy", "deadline:GetFleet", "deadline:GetQueueFleetAssociation", "deadline:ListFleets", "deadline:ListQueueFleetAssociations", "deadline:ListTagsForResource", "dms:DescribeDataMigrations", "dms:ListMigrationProjects", "glue:GetDataCatalogEncryptionSettings", "kafkaconnect:DescribeCustomPlugin", "kafkaconnect:DescribeWorkerConfiguration", "kafkaconnect:ListCustomPlugins", "kafkaconnect:ListTagsForResource", "kafkaconnect:ListWorkerConfigurations", "lakeformation:DescribeLakeFormationIdentityCenterConfiguration", "medialive:DescribeMultiplexProgram", "medialive:ListMultiplexPrograms", "mediapackagev2:GetChannelGroup", "mediapackagev2:ListChannelGroups", "rds:DescribeEngineDefaultParameters", | This policy now supports additional permissions for AWS ARC - Zonal Shift, Amazon Bedrock, AWS CloudTrail, AWS CodeArtifact, AWS Deadline Cloud, AWS Database Migration Service, AWS Glue, AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka, AWS Lake Formation, Amazon CloudWatch Logs, AWS Elemental MediaLive, AWS Elemental MediaPackage, Amazon Relational Database Service, Amazon Simple Storage Service, AWS Secrets Manager, Amazon Security Lake, AWS Service Catalog, Amazon Simple Email Service, and AWS X-Ray. | July 28, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| "rolesanywhere:GetProfile", "rolesanywhere:GetTrustAnchor", "rolesanywhere:ListProfiles", "rolesanywhere:ListTagsForResource", "rolesanywhere:ListTrustAnchors", "s3:GetAccessGrant", "s3:ListAccessGrants", "secretsmanager:DescribeSecret", "securitylake:ListDataLakeExceptions", "securitylake:ListDataLakes", "securitylake:ListLogSources", "servicecatalog:GetAttributeGroup", "servicecatalog:ListAttributeGroups", "servicecatalog:ListServiceActions", "servicecatalog:ListServiceActionsForProvisioningArtifact", "ses:GetTrafficPolicy", "ses:ListTagsForResource", "ses:ListTrafficPolicies", "xray:GetGroup", "xray:GetGroups", "xray:GetSamplingRules", "xray:ListResourcePolicies", "xray:ListTagsForResource" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add<br><br>"arc-zonal-shift:GetAutoshiftObserverNotificationStatus", "bedrock:GetModelInvocationLoggingConfiguration", "cloudtrail:GetEventConfiguration", "codeartifact:DescribeDomain", "codeartifact:GetDomainPermissionsPolicy", "deadline:GetFleet", "deadline:GetQueueFleetAssociation", "deadline:ListFleets", "deadline:ListQueueFleetAssociations", "deadline:ListTagsForResource", "dms:DescribeDataMigrations", "dms:ListMigrationProjects", "glue:GetDataCatalogEncryptionSettings", "iam:ListPolicies", "kafkaconnect:DescribeCustomPlugin", "kafkaconnect:DescribeWorkerConfiguration", "kafkaconnect:ListCustomPlugins", "kafkaconnect:ListTagsForResource", "kafkaconnect:ListWorkerConfigurations", "lakeformation:DescribeLakeFormationIdentityCenterConfiguration", "logs:DescribeIndexPolicies", "logs:ListTagsForResource", "medialive:DescribeMultiplexProgram", "medialive:ListMu | This policy now supports additional permissions for AWS ARC - Zonal Shift, Amazon Bedrock, AWS CloudTrail, AWS CodeArtifact, AWS Deadline Cloud, AWS Database Migration Service, AWS Glue, AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka, AWS Lake Formation, Amazon CloudWatch Logs, AWS Elemental MediaLive, AWS Elemental MediaPackage, Amazon Relational Database Service, Amazon Simple Storage Service, AWS Secrets Manager, Amazon Security Lake, AWS Service Catalog, Amazon Simple Email Service, AWS X-Ray, and Amazon API Gateway. | July 28, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| ltiplexPrograms", "mediapackagev2:GetChannelGroup", "mediapackagev2:ListChannelGroups", "rds:DescribeEngineDefaultParameters", "rolesanywhere:GetProfile", "rolesanywhere:GetTrustAnchor", "rolesanywhere:ListProfiles", "rolesanywhere:ListTagsForResource", "rolesanywhere:ListTrustAnchors", "s3:GetAccessGrant", "s3:ListAccessGrants", "secretsmanager:DescribeSecret", "securitylake:ListDataLakeExceptions", "securitylake:ListDataLakes", "securitylake:ListLogSources", "servicecatalog:GetAttributeGroup", "servicecatalog:ListAttributeGroups", "servicecatalog:ListServiceActions", "servicecatalog:ListServiceActionsForProvisioningArtifact", "ses:GetTrafficPolicy", "ses:ListTagsForResource", "ses:ListTrafficPolicies", "xray:GetGroup", "xray:GetGroups", "xray:GetSamplingRules", "xray:ListResourcePolicies", "xray:ListTagsForResource", "arn:aws:apigateway:::/account", "arn:aws:apigateway:::/ | | |

| Change | Description | Date |
| --- | --- | --- |
| usageplans", "arn:aws:apigateway:::/usageplans/". | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "backup-gateway:GetHypervisor", "backup-gateway:ListHypervisors", "bcm-data-exports:GetExport", "bcm-data-exports:ListExports", "bcm-data-exports:ListTagsForResource", "bedrock:GetAgent", "bedrock:GetAgentActionGroup", "bedrock:GetAgentKnowledgeBase", "bedrock:GetDataSource", "bedrock:GetFlowAlias", "bedrock:GetFlowVersion", "bedrock:ListAgentActionGroups", "bedrock:ListAgentKnowledgeBases", "bedrock:ListDataSources", "bedrock:ListFlowAliases", "bedrock:ListFlowVersions", "cloudformation:BatchDescribeTypeConfigurations", "cloudformation:DescribeStackInstance", "cloudformation:DescribeStackSet", "cloudformation:ListStackInstances", "cloudformation:ListStackSets", "cloudfront:GetPublicKey", "cloudfront:GetRealtimeLogConfig", "cloudfront:ListPublicKeys", "cloudfront:ListRealtimeLogConfigs", "entityre | This policy now supports additional permissions for AWS Backup gateway, AWS Billing and Cost Management, Amazon Bedrock, AWS CloudFormation, Amazon CloudFront, AWS Entity Resolution, AWS IoT Core Device Advisor, AWS Lambda, AWS Network Manager, AWS Private Certificate Authority, Amazon Relational Database Service, Amazon Redshift, Amazon S3 Tables, AWS Systems Manager Quick Setup. | June 18, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| solution:GetIdMappingWorkflow", "entityresolution:GetSchemaMapping", "entityresolution:ListIdMappingWorkflows", "entityresolution:ListSchemaMappings", "entityresolution:ListTagsForResource", "iotdeviceadvisor:GetSuiteDefinition", "iotdeviceadvisor:ListSuiteDefinitions", "lambda:GetEventSourceMapping", "lambda:ListEventSourceMappings", "mediapackagev2:GetChannel", "mediapackagev2:ListChannels", "networkmanager:GetTransitGatewayPeering", "networkmanager:ListPeerings", "pca-connector-ad:GetDirectoryRegistration", "pca-connector-ad:ListDirectoryRegistrations", "pca-connector-ad:ListTagsForResource", "rds:DescribeDBShardGroups", "rds:DescribeIntegrations", "redshift:DescribeIntegrations", "s3tables:GetTableBucket", "s3tables:GetTableBucketEncryption", "s3tables:GetTableBucketMaintenanceConfiguration", "s3tables:ListTableBuckets", "ssm-quicksetup:GetConfigurationManager", "ssm-qu | | |

| Change | Description | Date |
| --- | --- | --- |
| icksetup:ListConfigurationManagers" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "backup-gateway:GetHypervisor", "backup-gateway:ListHypervisors", "bcm-data-exports:GetExport", "bcm-data-exports:ListExports", "bcm-data-exports:ListTagsForResource", "bedrock:GetAgent", "bedrock:GetAgentActionGroup", "bedrock:GetAgentKnowledgeBase", "bedrock:GetDataSource", "bedrock:GetFlowAlias", "bedrock:GetFlowVersion", "bedrock:ListAgentActionGroups", "bedrock:ListAgentKnowledgeBases", "bedrock:ListDataSources", "bedrock:ListFlowAliases", "bedrock:ListFlowVersions", "cloudformation:BatchDescribeTypeConfigurations", "cloudformation:DescribeStackInstance", "cloudformation:DescribeStackSet", "cloudformation:ListStackInstances", "cloudformation:ListStackSets", "cloudfront:GetPublicKey", "cloudfront:GetRealtimeLogConfig", "cloudfront:ListPublicKeys", "cloudfront:ListRealtimeLogConfigs", "entityresolution:GetIdMapp | This policy now supports additional permissions for AWS Backup gateway, AWS Billing and Cost Management, Amazon Bedrock, AWS CloudFormation, Amazon CloudFront, AWS Entity Resolution, AWS IoT Core Device Advisor, AWS Lambda, AWS Network Manager, AWS Private Certificate Authority, Amazon Relational Database Service, Amazon Redshift, Amazon S3 Tables, AWS Systems Manager Quick Setup. | June 18, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| ingWorkflow", "entityresolution:GetSchemaMapping", "entityresolution:ListIdMappingWorkflows", "entityresolution:ListSchemaMappings", "entityresolution:ListTagsForResource", "iotdeviceadvisor:GetSuiteDefinition", "iotdeviceadvisor:ListSuiteDefinitions", "lambda:GetEventSourceMapping", "lambda:ListEventSourceMappings", "networkmanager:GetTransitGatewayPeering", "networkmanager:ListPeerings", "pca-connector-ad:GetDirectoryRegistration", "pca-connector-ad:ListDirectoryRegistrations", "pca-connector-ad:ListTagsForResource", "rds:DescribeDBShardGroups", "rds:DescribeIntegrations", "redshift:DescribeIntegrations", "s3tables:GetTableBucket", "s3tables:GetTableBucketEncryption", "s3tables:GetTableBucketMaintenanceConfiguration", "s3tables:ListTableBuckets", "ssm-quicksetup:GetConfigurationManager", "ssm-quicksetup:ListConfigurationManagers" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource" | This policy now supports additional permissions for Amazon Bedrock. | May 27, 2025 |
| AWSConfigServiceRolePolicy – Add "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource" | This policy now supports additional permissions for Amazon Bedrock. | May 27, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", | This policy now supports additional permissions for AWS B2B Data Interchange, Amazon Bedrock, AWS Clean Rooms, AWS CodeConnections, AWS Direct Connect, AWS Database Migration Service (AWS DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, AWS Security Hub CSPM, and AWS Systems Manager Incident Manager, AWS Systems Manager Incident Manager Contacts, and AWS Systems Manager. | April 08, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| "route53profiles:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", | This policy now supports additional permissions for AWS B2B Data Interchange, Amazon Bedrock, AWS Clean Rooms, AWS CodeConnections, AWS Direct Connect, AWS Database Migration Service (AWS DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, AWS Security Hub CSPM, and AWS Systems Manager Incident Manager, AWS Systems Manager Incident Manager Contacts, and AWS Systems Manager. This policy also now supports permission to access all Amazon API Gateway domain names by including the resource pattern `"arn:aws:apigateway:::/domainnames/ "`. | April 08, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| "route53profiles:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation" | | |
| AWS_ConfigRole – Add "ec2:GetAllowedImagesSettings" | This policy now supports additional permissions for Amazon Elastic Compute Cloud (Amazon EC2). | March 4, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "ec2:GetAllowedImagesSettings" | This policy now supports additional permissions for Amazon Elastic Compute Cloud (Amazon EC2). | March 4, 2025 |
| AWS_ConfigRole – Add "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools" | This policy now supports additional permissions for AWS Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2), AWS HealthOmics, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Email Service (Amazon SES). | January 16, 2025 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools" | This policy now supports additional permissions for AWS Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2), AWS HealthOmics, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Email Service (Amazon SES). | January 16, 2025 |
| AWSConfigServiceRolePolicy – Add "organizations:ListAWSServiceAccessForOrganization" | This policy now supports additional permissions for AWS Organizations. | December 18, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot | This policy now supports additional permissions for AWS AppConfig, AWS CloudTrail, Amazon Connect, Amazon DataZone, Amazon DevOps Guru, AWS Glue, Identity Store, AWS IoT, AWS IoT FleetWise, AWS IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, AWS Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler, AWS Systems Manager, and Amazon VPC Lattice. | November 7, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| :ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAnomalyDete | | |

| Change | Description | Date |
| --- | --- | --- |
| ctors", "oam:GetSink" "oam :GetSinkPolicy", "oam:List Sinks", "payment-cryptograp hy:GetAlias", "payment- cryptography:GetKey", "payment-cryptography:L istAliases", "payment-crypt ography:ListKeys", "payment -cryptography:ListTagsForRe source", "rds:DescribeDBPro xyTargetGroups", "rds:Desc ribeDBProxyTargets", "rekog nition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", " scheduler:GetScheduleGroup" , "scheduler:ListScheduleGrou ps", "scheduler:ListTagsFor Resource", "ssm:GetServiceSet ting", "vpc-lattice:GetAcce ssLogSubscription", "vpc-la ttice:GetService", "vpc-latt ice:GetServiceNetwork", "vp c-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogS ubscriptions", "vpc-lattice :ListServiceNetworks", "vpc- lattice:ListServices", "vpc-lat tice:ListTagsForResource", "vpc-lattice:ListTargetGrou ps", and "vpc-lattice:ListT argets" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", | This policy now supports additional permissions for AWS AppConfig, AWS CloudTrail, Amazon Connect, Amazon DataZone, Amazon DevOps Guru, AWS Glue, Identity Store, AWS IoT, AWS IoT FleetWise, AWS IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, AWS Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler, AWS Systems Manager, and Amazon VPC Lattice. | November 7, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| "iot:ListThingGroups", "iot:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", | | |

| Change | Description | Date |
| --- | --- | --- |
| "logs:ListLogAnomalyDetectors", "oam:GetSink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup," "iot:ListBillingGroups," "ivs:GetEncoderConfiguration," "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration," "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest | This policy now supports additional permissions for Amazon OpenSearch Service Severless, Amazon AppStream, AWS Backup, AWS CloudTrail, AWS Glue, EC2 Image Builder, AWS IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTailor, AWS HealthOmics, and Amazon EventBridge Scheduler. | September 16, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| rictionPolicies," "ivs:List Stages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup," "iot:ListBillingGroups," "ivs:GetEncoderConfiguration," "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration," "ivs:ListEncoderConfigurations," "ivs:ListPla | This policy now supports additional permissions for Amazon OpenSearch Service Severless, Amazon AppStream, AWS Backup, AWS CloudTrail, AWS Glue, EC2 Image Builder, AWS IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTailor, AWS HealthOmics, and Amazon EventBridge Scheduler. | September 16, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| ybackRestrictionPolicies," "ivs:ListStages," "ivs:List StorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:List Bridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules" | | |
| AWS_ConfigRole – Add "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource" | This policy now supports additional permissions for Amazon Elastic File System (Amazon EFS), Amazon Redshift and AWS Systems Manager for SAP. | June 17, 2024 |
| AWSConfigServiceRolePolicy – Add "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource" | This policy now supports additional permissions for Amazon Elastic File System (Amazon EFS), Amazon Redshift and AWS Systems Manager for SAP. | June 17, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:GetSMSSandboxAccountStatus" | This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, AWS Glue, AWS Identity and Access Management (IAM), AWS Lambda, AWS RAM, Amazon Redshift Serverless, Amazon SageMaker AI, and Amazon Simple Notification Service (Amazon SNS). | February 22, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInference | This policy now supports additional permissions for Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, AWS Glue, AWS Identity and Access Management (IAM), AWS Lambda, AWS RAM, Amazon Redshift Serverless, Amazon SageMaker AI, and Amazon Simple Notification Service (Amazon SNS). | February 22, 2024 |

| Change | Description | Date |
| --- | --- | --- |
| Experiments," and "sns:GetSMSSandboxAccountStatus" | | |
| AWSConfigUserAccess – AWS Config starts tracking changes for this AWS managed policy | This policy provides access to use AWS Config, including searching by tags on resources and reading all tags. This does not provide permission to configure AWS Config, which requires administrative privileges. | February 22, 2024 |
| AWS_ConfigRole – Add "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets" | This policy now supports additional permissions for AWS AppConfig, Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs, AWS Organizations, and Amazon Simple Storage Service (Amazon S3). | Decemeber 5, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets" | This policy now supports additional permissions for AWS AppConfig, Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs, AWS Organizations, and Amazon Simple Storage Service (Amazon S3). | December 5, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationAssociation | This policy now supports additional permissions for Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station, AWS Mainframe Modernization, Amazon MemoryDB, AWS Organizations, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53, AWS Service Catalog, and AWS Transfer Family. | November 17, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| s," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrL | | |

| Change | Description | Date |
| --- | --- | --- |
| ocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles" | | |
| AWS_ConfigRole – Add "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID" | This policy now adds security identifiers (SID) for `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , and `AWSConfigSLRApiGatewayStatementID` . | November 17, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect | This policy now supports additional permissions for Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station, AWS Mainframe Modernization, Amazon MemoryDB, AWS Organizations, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53, AWS Service Catalog, and AWS Transfer Family. | November 17, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| :ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid | | |

| Change | Description | Date |
| --- | --- | --- |
| rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles" | | |
| AWSConfigServiceRolePolicy – Add "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID" | This policy now adds security identifiers (SID) for `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , and `AWSConfigSLRApiGatewayStatementID` . | November 17, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT | This policy now supports additional permissions for AWS Private CA, AWS App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty, Amazon Inspector, AWS IoT, AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK), AWS Lambda, AWS Network Manager, AWS Organizations, and Amazon SageMaker AI. | October 4, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi | This policy now supports additional permissions for AWS Private CA, AWS App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty, Amazon Inspector, AWS IoT, AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK), AWS Lambda, AWS Network Manager, AWS Organizations, and Amazon SageMaker AI. | October 4, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob" | | |
| AWSConfigServiceRolePolicy – Remove "ssm:GetParameter" | This policy now removes permissions for AWS Systems Manager (Systems Manager). | September 6, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe | This policy now supports additional permissions for AWS App Mesh, AWS CloudFormation, Amazon CloudFront AWS CodeArtifact, AWS CodeBuild, Amazon Connect, AWS Glue, Amazon GuardDuty, AWS Identity and Access Management (IAM), Amazon Inspector, AWS IoT, AWS IoT TwinMaker, AWS IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, AWS Network Manager, AWS Organizations, AWS Resource Explorer, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Notification Service (Amazon SNS). | July 28, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe | This policy now supports additional permissions for AWS App Mesh, Amazon WorkSpaces Applications, AWS CloudFormation, Amazon CloudFront, AWS CodeArtifact, AWS CodeBuild, Amazon Connect, AWS Glue, Amazon GuardDuty, AWS Identity and Access Management (IAM), Amazon Inspector, AWS IoT, AWS IoT TwinMaker, AWS IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, AWS Network Manager, AWS Organizations, AWS Resource Explorer, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), and Amazon EC2 Systems Manager (SSM). | July 28, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa | This policy now supports additional permissions for AWS Amplify, Amazon Connect, AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, AWS Batch, AWS CloudFormation, AWS CloudTrail, AWS CodeArtifact, Amazon CodeGuru, AWS Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, AWS Organizations, Amazon Forecast, AWS IoT Greengrass, AWS Ground Station, AWS Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon Quick Suite, AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, AWS Transfer Family. | June 13, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| tasetGroup", "forecast :ListDatasetGroups", "greeng rass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVe rsions", "groundstation:GetM issionProfile", "groundstati on:ListMissionProfiles", "iam:ListGroups", "iam:ListR oles", "kafka:DescribeCon figuration", "kafka:Describe ConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDat abases" "logs:ListTagsLogG roup", "mediaconnec t:DescribeFlow", "mediacon nect:ListFlows", "mediatailo r:GetPlaybackConfiguration" , "mediatailor:ListPlaybackC onfigurations", "mobiletarge ting:GetApplicationSettings ", "mobiletargeting:GetEmail Template", "mobiletargeting: GetEventStream", "mobileta rgeting:ListTemplates", "networkmanager:GetCus tomerGatewayAssociations", "networkmanager:Get LinkAssociations", "organiza tions:DescribeAccount", "organizations:Describ eOrganizationalUnit", "organizations:ListAccou | | |

| Change | Description | Date |
| --- | --- | --- |
| nts", "organizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast | This policy now supports additional permissions for AWS Amplify, Amazon Connect, AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, AWS Batch, AWS CloudFormation, AWS CloudTrail, AWS CodeArtifact, Amazon CodeGuru, AWS Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, AWS Organizations,Amazon Forecast, AWS IoT Greengrass, AWS Ground Station, AWS Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon Quick Suite, AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, AWS Transfer Family. | June 13, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:Lis | | |

| Change | Description | Date |
| --- | --- | --- |
| tAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource" | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedD | This policy now supports additional permissions for Amazon Managed Workflows for AWS Amplify, AWS App Mesh, AWS App Runner, Amazon CloudFront, AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, AWS Transfer Family, Amazon Pinpoint, AWS Migration Hub, AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service, and AWS WAF. | April 13, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| iscoveryConfiguration, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie | This policy now supports additional permissions for Amazon Managed Workflows for AWS Amplify, AWS App Mesh, AWS App Runner, Amazon CloudFront, AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, AWS Transfer Family, Amazon Pinpoint, AWS Migration Hub, AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service, and AWS WAF. | April 13, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| 2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam: | This policy now supports additional permissions for Amazon Managed Workflows for Amazon AppFlow, AWS App Runner, Amazon WorkSpaces Applications, Amazon CloudFront, Amazon CloudWatch, AWS CodeArtifact, AWS CodeCommit, AWS Device Farm, Amazon CloudWatch Evidently, Amazon Forecast, AWS Ground Station, AWS Identity and Access Management (IAM), AWS IoT, Amazon MemoryDB, Amazon Pinpoint, AWS Network Manager, AWS Panorama, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon SageMaker AI. | March 30, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, | This policy now supports additional permissions for Amazon Managed Workflows for Amazon AppFlow, AWS App Runner, Amazon WorkSpaces Applications, AWS CloudFormation, Amazon CloudFront, Amazon CloudWatch, AWS CodeArtifact, AWS CodeCommit, AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Ground Station, AWS Identity and Access Management (IAM), AWS IoT, Amazon MemoryDB, Amazon Pinpoint, AWS Network Manager, AWS Panorama, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon SageMaker AI. | March 30, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, network manager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigRulesExecutionRole – AWS Config starts tracking changes for this AWS managed policy | This policy allow AWS Lambda functions to access the AWS Config API and the configuration snapshots that AWS Config delivers periodically to Amazon S3. This access is required by functions that evaluate configuration changes for AWS Custom Lambda rules. | March 7, 2023 |
| AWSConfigRoleForOrganizations – AWS Config starts tracking changes for this AWS managed policy | This policy allows AWS Config to call read-only AWS Organizations APIs. | March 7, 2023 |
| AWSConfigRemediationServiceRolePolicy – AWS Config starts tracking changes for this AWS managed policy | This policy allows AWS Config to remediate `NON_COMPLIANT` resources on your behalf. | March 7, 2023 |
| AWSConfigServiceRolePolicy – Add auditmanager:GetAccountStatus | This policy now grants permission to return the registration status of an account in AWS Audit Manager. | March 3, 2023 |
| AWS_ConfigRole – Add auditmanager:GetAccountStatus | This policy now grants permission to return the registration status of an account in AWS Audit Manager. | March 3, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigMultiAccountSetupPolicy – AWS Config starts tracking changes for this AWS managed policy | This policy allows AWS Config to call AWS services and deploy AWS Config resources across an organization with AWS Organizations. | February 27, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar | This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs. | February 1, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar | This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs. | February 1, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries | | |
| ConfigConformsServiceRolePolicy – Update config:DescribeConfigRules | As a security best practice, this policy now removes broad resource-level permission for `config:DescribeConfigRules` . | January 12, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, | This policy now supports additional permissions for Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon Quick Suite, AWS Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream. | Decemeber 15, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:D | This policy now supports additional permissions for Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon Quick Suite, AWS Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream. | Decemeber 15, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| escribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add cloudformation:ListStackResources and cloudformation:ListStacks | This policy now grants permission to return descriptions of all resources of a specified AWS CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter. | November 7, 2022 |
| AWS_ConfigRole – Add cloudformation:ListStackResources and cloudformation:ListStacks | This policy now grants permission to return descriptions of all resources of a specified AWS CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter. | November 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers | This policy now supports additional permissions for AWS Certificate Manager, Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map, and AWS Security Token Service. | October 19, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, | | |

| Change | Description | Date |
| --- | --- | --- |
| iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, io tsitewise:ListProjectAssets , iotsitewise:ListProjects, i otsitewise:ListTagsForResou rce, iotwireless:GetSer viceProfile, iotwireless:Ge tWirelessDevice, iotwireles s:GetWirelessGatewayTaskDef inition, iotwireless:ListSe rviceProfiles, iotwireless: ListTagsForResource, iotwir eless:ListWirelessDevices, iotwireless:ListWirelessGat ewayTaskDefinitions, lex:De scribeBotVersion, lex:ListB otVersions, lightsail:GetCo ntainerServices, lightsail :GetDistributions, lightsai l:GetRelationalDatabase, li ghtsail:GetRelationalDataba seParameters, mobiletargeti ng:GetApps, mobiletar geting:GetCampaign, mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeAp plicationInstance, panorama :DescribeApplicationInstanc | | |

| Change | Description | Date |
| --- | --- | --- |
| eDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers | This policy now supports additional permissions for AWS Certificate Manager, Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map, and AWS Security Token Service. | October 19, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, | | |

| Change | Description | Date |
| --- | --- | --- |
| iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanc | | |

| Change | Description | Date |
| --- | --- | --- |
| eDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add Glue::GetTable | This policy now grants permission to retrieve the AWS Glue Table definition in a Data Catalog for a specified table. | September 14, 2022 |
| AWS_ConfigRole – Add Glue::GetTable | This policy now grants permission to retrieve the AWS Glue Table definition in a Data Catalog for a specified table. | September 14, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte | This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick Suite, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage | September 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:Descr | Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer, AWS Cloud9, AWS Directory Service, AWS DataSync, AWS Elemental MediaPackage, AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, and AWS Transfer Family. | |

| Change | Description | Date |
| --- | --- | --- |
| ibeFleetCapacity, gamelift: DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift: ListFleets, gamelift:ListGameServerGroups, gamelift: ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimensio | | |

| Change | Description | Date |
| --- | --- | --- |
| n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:Descri | | |

| Change | Description | Date |
| --- | --- | --- |
| beAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarm | | |

| Change | Description | Date |
| --- | --- | --- |
| s, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStati cIp, lightsail:GetStaticIps, lookoutequipment:Describe InferenceScheduler, lookout equipment:ListTagsForResour ce, lookoutmetrics:Describe Alert, lookoutmetrics:Descr ibeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyD etectors, lookoutmetrics:Li stMetricSets, lookoutmetric s:ListTagsForResource, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage- vod:ListPackagingGroups, | | |

| Change | Description | Date |
| --- | --- | --- |
| mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:De | | |

| Change | Description | Date |
| --- | --- | --- |
| scribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, | | |

| Change | Description | Date |
| --- | --- | --- |
| rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:Describ | | |

| Change | Description | Date |
| --- | --- | --- |
| eTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets, ec2:G | This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick Suite, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage | September 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| etNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttrib | Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer, AWS Cloud9, AWS Directory Service, AWS DataSync, AWS Elemental MediaPackage, AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, and AWS Transfer Family | |

| Change | Description | Date |
| --- | --- | --- |
| utes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, | | |

| Change | Description | Date |
| --- | --- | --- |
| iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAs | | |

| Change | Description | Date |
| --- | --- | --- |
| sets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, | | |

| Change | Description | Date |
| --- | --- | --- |
| lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobilet | | |

| Change | Description | Date |
| --- | --- | --- |
| argeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, res | | |

| Change | Description | Date |
| --- | --- | --- |
| iliencehub:ListAppVersionResourceMappings, resilienceh ub:ListResiliencyPolicies, route53-recovery-readiness: GetCell, route53-recovery-r eadiness:GetReadinessCheck, route53-recovery-readiness :GetRecoveryGroup, route53-recovery-readiness:GetResou rceSet, route53-recovery-re adiness:ListCells, route53-recovery-readiness:ListRead inessChecks, route53-recove ry-readiness:ListRecoveryGr oups, route53-recovery-readiness:ListResource Sets, route53resolver:GetFi rewallDomainList, route53re solver:GetFirewallRuleGroup , route53resolver:GetFirewa llRuleGroupAssociation, route53resolver:GetRe solverQueryLogConfig, route 53resolver:ListFirewallDoma inLists, route53resolver:Li stFirewallDomains, route53r esolver:ListFirewallRuleGro upAssociations, route53reso lver:ListFirewallRuleGroups , route53resolver:ListFirew allRules, route53resolver:L istResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:Li | | |

| Change | Description | Date |
| --- | --- | --- |
| stTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTab | | |

| Change | Description | Date |
| --- | --- | --- |
| les, timestream:ListTagsFor Resource, transfer:DescribeS erver, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer: ListUsers, transfer:ListWor kflows, voiceid:DescribeDo main, and voiceid:ListTa gsForResource | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar | This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs. | February 1, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar | This policy now supports additional permissions for Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs. | February 1, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries | | |
| ConfigConformsServiceRolePolicy – Update config:DescribeConfigRules | As a security best practice, this policy now removes broad resource-level permission for `config:DescribeConfigRules` . | January 12, 2023 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, | This policy now supports additional permissions for Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon Quick Suite, AWS Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream. | Decemeber 15, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:D | This policy now supports additional permissions for Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon Quick Suite, AWS Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream. | December 15, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| escribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add cloudformation:ListStackResources and cloudformation:ListStacks | This policy now grants permission to return descriptions of all resources of a specified AWS CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter. | November 7, 2022 |
| AWS_ConfigRole – Add cloudformation:ListStackResources and cloudformation:ListStacks | This policy now grants permission to return descriptions of all resources of a specified AWS CloudFormation stack and return the summary information for stacks whose status matches the specified StackStatusFilter. | November 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers | This policy now supports additional permissions for AWS Certificate Manager, Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map, and AWS Security Token Service. | October 19, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, | | |

| Change | Description | Date |
| --- | --- | --- |
| iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanc | | |

| Change | Description | Date |
| --- | --- | --- |
| eDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers | This policy now supports additional permissions for AWS Certificate Manager, Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map, and AWS Security Token Service. | October 19, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, | | |

| Change | Description | Date |
| --- | --- | --- |
| iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, io tsitewise:ListProjectAssets , iotsitewise:ListProjects, i otsitewise:ListTagsForResou rce, iotwireless:GetSer viceProfile, iotwireless:Ge tWirelessDevice, iotwireles s:GetWirelessGatewayTaskDef inition, iotwireless:ListSe rviceProfiles, iotwireless: ListTagsForResource, iotwir eless:ListWirelessDevices, iotwireless:ListWirelessGat ewayTaskDefinitions, lex:De scribeBotVersion, lex:ListB otVersions, lightsail:GetCo ntainerServices, lightsail :GetDistributions, lightsai l:GetRelationalDatabase, li ghtsail:GetRelationalDataba seParameters, mobiletargeti ng:GetApps, mobiletar geting:GetCampaign, mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeAp plicationInstance, panorama :DescribeApplicationInstanc | | |

| Change | Description | Date |
| --- | --- | --- |
| eDetails, panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add Glue::GetTable | This policy now grants permission to retrieve the AWS Glue Table definition in a Data Catalog for a specified table. | September 14, 2022 |
| AWS_ConfigRole – Add Glue::GetTable | This policy now grants permission to retrieve the AWS Glue Table definition in a Data Catalog for a specified table. | September 14, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte | This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick Suite, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage | September 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:Descr | Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer, AWS Cloud9, AWS Directory Service, AWS DataSync, AWS Elemental MediaPackage, AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, and AWS Transfer Family. | |

| Change | Description | Date |
| --- | --- | --- |
| ibeFleetCapacity, gamelift: DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift: ListFleets, gamelift:ListGameServerGroups, gamelift: ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimensio | | |

| Change | Description | Date |
| --- | --- | --- |
| n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:Descri | | |

| Change | Description | Date |
| --- | --- | --- |
| beAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarm | | |

| Change | Description | Date |
| --- | --- | --- |
| s, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStati cIp, lightsail:GetStaticIps, lookoutequipment:Describe InferenceScheduler, lookout equipment:ListTagsForResour ce, lookoutmetrics:Describe Alert, lookoutmetrics:Descr ibeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyD etectors, lookoutmetrics:Li stMetricSets, lookoutmetric s:ListTagsForResource, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage-vod:ListPackagingGroups, | | |

| Change | Description | Date |
| --- | --- | --- |
| mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:De | | |

| Change | Description | Date |
| --- | --- | --- |
| scribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, | | |

| Change | Description | Date |
| --- | --- | --- |
| rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:Describ | | |

| Change | Description | Date |
| --- | --- | --- |
| eTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets, ec2:G | This policy now supports additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick Suite, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, Amazon Simple Storage | September 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| etNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttrib | Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer, AWS Cloud9, AWS Directory Service, AWS DataSync, AWS Elemental MediaPackage, AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, and AWS Transfer Family | |

| Change | Description | Date |
| --- | --- | --- |
| utes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, | | |

| Change | Description | Date |
| --- | --- | --- |
| iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAs | | |

| Change | Description | Date |
| --- | --- | --- |
| sets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, | | |

| Change | Description | Date |
| --- | --- | --- |
| lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStati cIp, lightsail:GetStaticIps, lookoutequipment:Describe InferenceScheduler, lookout equipment:ListTagsForResour ce, lookoutmetrics:Describe Alert, lookoutmetrics:Descr ibeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyD etectors, lookoutmetrics:Li stMetricSets, lookoutmetric s:ListTagsForResource, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage- vod:ListPackagingGroups, mediapackage-vod:L istTagsForResource, mobilet | | |

| Change | Description | Date |
| --- | --- | --- |
| argeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, res | | |

| Change | Description | Date |
| --- | --- | --- |
| iliencehub:ListAppVersionResourceMappings, resilienceh ub:ListResiliencyPolicies, route53-recovery-readiness: GetCell, route53-recovery-r eadiness:GetReadinessCheck, route53-recovery-readiness :GetRecoveryGroup, route53-recovery-readiness:GetResou rceSet, route53-recovery-re adiness:ListCells, route53-recovery-readiness:ListRead inessChecks, route53-recove ry-readiness:ListRecoveryGr oups, route53-recovery-readiness:ListResource Sets, route53resolver:GetFi rewallDomainList, route53re solver:GetFirewallRuleGroup , route53resolver:GetFirewa llRuleGroupAssociation, route53resolver:GetRe solverQueryLogConfig, route 53resolver:ListFirewallDoma inLists, route53resolver:Li stFirewallDomains, route53r esolver:ListFirewallRuleGro upAssociations, route53reso lver:ListFirewallRuleGroups , route53resolver:ListFirew allRules, route53resolver:L istResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:Li | | |

| Change | Description | Date |
| --- | --- | --- |
| stTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTab | | |

| Change | Description | Date |
| --- | --- | --- |
| les, timestream:ListTagsFor Resource, transfer:DescribeS erver, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer: ListUsers, transfer:ListWor kflows, voiceid:DescribeDo main, and voiceid:ListTa gsForResource | | |
| AWSConfigServiceRolePolicy – Add datasync:ListAgent s, datasync:ListLocations, datasync:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists | This policy now grants permission to return a list of AWS DataSync agents, DataSync source and destinati on locations, and DataSync tasks in an AWS account; list summary information about the AWS Cloud Map namesp aces and services that are associated with one or more specified namespaces in an AWS account; and list all the Amazon Simple Email Service (Amazon SES) contact lists available in AWS account. | August 22, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists | This policy now grants permission to return a list of AWS DataSync agents, DataSync source and destination locations, and DataSync tasks in an AWS account; list summary information about the AWS Cloud Map namespaces and services that are associated with one or more specified namespaces in an AWS account; and list all the Amazon Simple Email Service (Amazon SES) contact lists available in AWS account. | August 22, 2022 |
| ConfigConformsServiceRolePolicy – Add cloudwatch:PutMetricData | This policy now grants permission to publish metric data points to Amazon CloudWatch. | July 25, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio | This policy now supports additional permissions for Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon Quick Suite, Amazon Rekognition, AWS RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES), AWS Amplify, AWS AppConfig, AWS AppSync, AWS Billing Conductor, AWS DataSync, AWS Firewall Manager, AWS Glue, AWS IAM Identity Center (IAM Identity Center), EC2 Image Builder, and Elastic Load Balancing. | July 15, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: List | | |

| Change | Description | Date |
| --- | --- | --- |
| ComponentBuildVersions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder: ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and | | |

| Change | Description | Date |
| --- | --- | --- |
| sso:GetInlinePolicyForPermissionSet | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De | This policy now supports additional permissions for Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon Quick Suite, Amazon Rekognition, AWS RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES), AWS Amplify, AWS AppConfig, AWS AppSync, AWS Billing Conductor, AWS DataSync, AWS Firewall Manager, AWS Glue, AWS IAM Identity Center (IAM Identity Center), EC2 Image Builder, and Elastic Load Balancing. | July 15, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| scribeLocationS3, datasync: DescribeLocationSmb, datasy nc:DescribeTask, datasync: ListTagsForResource, ecr:De scribePullThroughCacheRules , ecr:DescribeRegistry, ecr:G etRegistryPolicy, elasticac he:DescribeCacheParameters, elasticloadbalancing:Descr ibeListenerCertificates, el asticloadbalancing:Describe TargetGroupAttributes, elas ticloadbalancing:DescribeTa rgetGroups, elasticloadbala ncing:DescribeTargetHealth, events:DescribeApiDestinat ion, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListP olicies, fms:ListTagsForRes ource, fsx:DescribeVolumes, geo:DescribeGeofenceColl ection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator , geo:DescribeTracker, geo:ListTrackerConsumers, g lue:BatchGetJobs, glue:Batc hGetWorkflows, glue:GetC rawler, glue:GetCrawlers, glue:GetJob, glue:GetJ obs, glue:GetWorkflow, imagebuilder: GetCompon ent, imagebuilder: List ComponentBuildVersions, | | |

| Change | Description | Date |
| --- | --- | --- |
| imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and | | |

| Change | Description | Date |
| --- | --- | --- |
| sso:GetInlinePolicyForPermissionSet | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:DescribePer | This policy now grants permission to get a specified Amazon Athena data catalog, list the Athena data catalogs in an AWS account, and list tags associated with an Athena workgroup or data catalog resource; to get a list of Amazon Detective behavior graphs and list tags for a Detective behavior graph; get a list of resource metadata for a given list of AWS Glue development endpoint names, get information about a specified AWS Glue development endpoint, get all the AWS Glue development endpoints in an AWS account, retrieve a specified AWS Glue security configuration, get all AWS Glue security configurations, get a list of tags associated with an AWS Glue resource, get information about an AWS Glue workgroup with the specified name, retrieve the names of all AWS Glue crawler resources in an AWS account, get the names of all AWS Glue `DevEndpoint` resources in an AWS account, list the names of all | May 31, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| missionSet, sso:ListManaged PoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource | AWS Glue job resources in an AWS account, get details about AWS Glue member accounts, list names of AWS Glue workflows created in an account, and list available AWS Glue workgroups for an account; to retrieve details about an Amazon GuardDuty filter, retrieve a GuardDuty IPSet, retrieve a GuardDuty ThreatInt elSet, retrieve GuardDuty member accounts, get a list of GuardDuty filters, get the IPSets of the GuardDuty service, retrieve tags for the GuardDuty Service, and get the ThreatIntelSets of the GuardDuty service; to get the current status and configuration settings for an Amazon Macie acco unt; to retrieve the resource and principal associations for AWS Resource Access Manager (AWS RAM) resource shares and retrieve details about AWS RAM resource shares; to get information about an Amazon Simple Email Service (Amazon SES) existing configuration set, get a list of event destinati ons that are associated with | |

| Change | Description | Date |
| --- | --- | --- |
| | an Amazon SES configuration set, and list all of the configuration sets associated with an Amazon SES account; and to get a list of Identity Center directory attributes, get the details of an AWS IAM Identity Center permission set, get the IAM managed policy that is attached to a specified IAM Identity Center permission set, get the permissions set for an IAM Identity Center instance, and get tags for IAM Identity Center resources. | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:DescribePer | This policy now grants permission to get a specified Amazon Athena data catalog, list the Athena data catalogs in an AWS account, and list tags associated with an Athena workgroup or data catalog resource; to get a list of Amazon Detective behavior graphs and list tags for a Detective behavior graph; get a list of resource metadata for a given list of AWS Glue development endpoint names, get information about a specified AWS Glue development endpoint, get all the AWS Glue development endpoints in an AWS account, retrieve a specified AWS Glue security configuration, get all AWS Glue security configurations, get a list of tags associated with an AWS Glue resource, get information about an AWS Glue workgroup with the specified name, retrieve the names of all AWS Glue crawler resources in an AWS account, get the names of all AWS Glue `DevEndpoint` resources in an AWS account, list the names of all | May 31, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| missionSet, sso:ListManaged PoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource | AWS Glue job resources in an AWS account, get details about AWS Glue member accounts, list names of AWS Glue workflows created in an account, and list available AWS Glue workgroups for an account; to retrieve details about an Amazon GuardDuty filter, retrieve a GuardDuty IPSet, retrieve a GuardDuty ThreatInt elSet, retrieve GuardDuty member accounts, get a list of GuardDuty filters, get the IPSets of the GuardDuty service, retrieve tags for the GuardDuty Service, and get the ThreatIntelSets of the GuardDuty service; to get the current status and configuration settings for an Amazon Macie acco unt; to retrieve the resource and principal associations for AWS Resource Access Manager (AWS RAM) resource shares and retrieve details about AWS RAM resource shares; to get information about an Amazon Simple Email Service (Amazon SES) existing configuration set, get a list of event destinati ons that are associated with | |

| Change | Description | Date |
| --- | --- | --- |
| | an Amazon SES configuration set, and list all of the configuration sets associated with an Amazon SES account; and to get a list of Identity Center directory attributes, get the details of an AWS IAM Identity Center permission set, get the IAM managed policy that is attached to a specified IAM Identity Center permission set, get the permissions set for an IAM Identity Center instance, and get tags for IAM Identity Center resources. | |
| AWSConfigServiceRolePolicy – Add cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies | This policy now grants permission to get information about all or a specified AWS CloudTrail event data store (EDS), get information about all or a specified AWS CloudFormation resource, get a list of a DynamoDB Accelerator (DAX) parameter group or subnet group, get information about AWS Database Migration Service (AWS DMS) replication tasks for your account in the current region being accessed, and get a list all policies in an AWS Organizations of a specified type. | April 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies | This policy now grants permission to get information about all or a specified AWS CloudTrail event data store (EDS), get information about all or a specified AWS CloudFormation resource, get a list of a DynamoDB Accelerator (DAX) parameter group or subnet group, get information about AWS Database Migration Service (AWS DMS) replication tasks for your account in the current region being accessed, and get a list all policies in an AWS Organizations of a specified type. | April 7, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara | This policy now supports additional permissions for AWS Backup, AWS Batch, DynamoDB Accelerator, AWS Database Migration Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon GuardDuty, AWS Key Management Service, AWS OpsWorks, Amazon Relational Database Service, AWS WAFV2, and Amazon WorkSpaces. | March 14, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces | | |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct | This policy now supports additional permissions for AWS Backup, AWS Batch, DynamoDB Accelerator, AWS Database Migration Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon GuardDuty, AWS Key Management Service, AWS OpsWorks, Amazon Relational Database Service, AWS WAFV2, and Amazon WorkSpaces. | March 14, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces | | |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies | This policy now grants permission to get details about Elastic Beanstalk environments and a description of the settings for the specified Elastic Beanstalk configuration set, get a map of OpenSearch or Elasticsearch versions, describe the available Amazon RDS option groups for a database, and get information about a CodeDeploy deployment configuration. This policy also now grants permission to retrieve the specified alternate contact attached to an AWS account, retrieve information about an AWS Organizations policy, retrieve an Amazon ECR repository policy, retrieve information about an archived AWS Config rule, retrieve a list of Amazon ECS task definition families, list the root or parent organizational units (OUs) of the specified child OU or account, and list the policies that are attached to the specified target root, organizational unit, or account. | February 10, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies | This policy now grants permission to get details about Elastic Beanstalk environments and a description of the settings for the specified Elastic Beanstalk configuration set, get a map of OpenSearch or Elasticsearch versions, describe the available Amazon RDS option groups for a database, and get information about a CodeDeploy deployment configuration. This policy also now grants permission to retrieve the specified alternate contact attached to an AWS account, retrieve information about an AWS Organizations policy, retrieve an Amazon ECR repository policy, retrieve information about an archived AWS Config rule, retrieve a list of Amazon ECS task definition families, list the root or parent organizational units (OUs) of the specified child OU or account, and list the policies that are attached to the specified target root, organizational unit, or account. | February 10, 2022 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent | This policy now grants permission to create Amazon CloudWatch log groups and streams and to write logs to created log streams. | December 15, 2021 |
| AWS_ConfigRole – Add logs: CreateLogStream, logs:Crea teLogGroup, and logs: PutLogEvent | This policy now grants permission to create Amazon CloudWatch log groups and streams and to write logs to created log streams. | Decemeber 15, 2021 |
| AWSConfigServiceRolePolicy – Add es:DescribeDomain, es:DescribeDomains, rds:Des cribeDBParameters, and, elas ticache:DescribeSnapshots | This policy now grants permission to get details about an Amazon OpenSearc h Service (OpenSearch Service) domain/domains and to get a detailed parameter list for a particular Amazon Relational Database Service (Amazon RDS) DB parameter group. This policy also grant s permission to get detais about Amazon ElastiCache snapshots. | September 8, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots | This policy now grants permission to get details about an Amazon OpenSearch Service (OpenSearch Service) domain/domains and to get a detailed parameter list for a particular Amazon Relational Database Service (Amazon RDS) DB parameter group. This policy also grants permission to get detais about Amazon ElastiCache snapshots. | September 8, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine, and additional permissions for AWS resource types | This policy now grants permission to list tags for a log group, list tags for a state machine, and list all state machines. This policy now grants permission to get details about a state machine. This policy also now supports additional permissions for Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service, AWS Database Migration Service, AWS Global Accelerator, and AWS Storage Gateway. | July 28, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add logs: ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine, and additional permissions for AWS resource types | This policy now grants permission to list tags for a log group, list tags for a state machine, and list all state machines. This policy now grants permission to get details about a state machine. This policy also now supports additional permissions for Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service, AWS Database Migration Service, AWS Global Accelerator, and AWS Storage Gateway. | July 28, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add ssm:DescribeDocumentPermission and additional permissions for AWS resource types | This policy now grants permission to view the permissions of AWS Systems Manager documents and information about IAM Access Analyzer. This policy now supports additional AWS resource types for Amazon Kinesis, Amazon ElastiCache, Amazon EMR, AWS Network Firewall, Amazon Route 53, and Amazon Relational Database Service (Amazon RDS). These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types. This policy also now support filtering Lambda@Edge functions for the lambda-inside-vpc AWS Config managed rule. | June 8, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add ssm:DescribeDocumentPermission and additional permissions for AWS resource types | This policy now grants permission to view the permissions of AWS Systems Manager documents and information about IAM Access Analyzer. This policy now supports additional AWS resource types for Amazon Kinesis, Amazon ElastiCache, Amazon EMR, AWS Network Firewall, Amazon Route 53, and Amazon Relational Database Service (Amazon RDS). These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types. This policy also now support filtering Lambda@Edge functions for the lambda-inside-vpc AWS Config managed rule. | June 8, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add apigateway:GET permission to make read-only GET calls to API Gateway and s3:GetAccessPointPolicy permission and s3:GetAccessPointPolicyStatus permission to invoke Amazon S3 read-only APIs | This policy now grants permissions that allow AWS Config to make read-only GET calls to API Gateway to support a AWS Config Rule for API Gateway. The policy also adds permissions that allow AWS Config to invoke Amazon Simple Storage Service (Amazon S3) read-only APIs, which are required to support the new `AWS::S3::AccessPoint` resource type. | May 10, 2021 |
| AWS_ConfigRole – Add apigateway:GET permission to make read-only GET calls to API Gateway and s3:GetAccessPointPolicy permission and s3:GetAccessPointPolicyStatus permission to invoke Amazon S3 read-only APIs | This policy now grants permissions that allow AWS Config to make read-only GET calls to API Gateway to support a AWS Config for API Gateway. The policy also adds permissions that allow AWS Config to invoke Amazon Simple Storage Service (Amazon S3) read-only APIs, which are required to support the new `AWS::S3::AccessPoint` resource type. | May 10, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWSConfigServiceRolePolicy – Add ssm:ListDocuments permission and additional permissions for AWS resource types | This policy now grants permission to view informati on about AWS Systems Manager specified documents . This policy also now supports additional AWS resource types for AWS Backup, Amazon Elastic File System, Amazon ElastiCac he, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon SageMaker AI, AWS Database Migration Service, and Amazon Route 53. These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types. | April 1, 2021 |

| Change | Description | Date |
| --- | --- | --- |
| AWS_ConfigRole – Add ssm:ListDocuments permission and additional permissions for AWS resource types | This policy now grants permission to view information about AWS Systems Manager specified documents. This policy also now supports additional AWS resource types for AWS Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon SageMaker AI, AWS Database Migration Service, and Amazon Route 53. These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types. | April 1, 2021 |
| `AWSConfigRole` is deprecated | `AWSConfigRole` is deprecated. The replacement policy is `AWS_ConfigRole`. | April 1, 2021 |
| AWS Config started tracking changes | AWS Config started tracking changes for its AWS managed policies. | April 1, 2021 |

## Permissions for the IAM Role Assigned to AWS Config

An IAM role lets you define a set of permissions. AWS Config assumes the role that you assign to it to write to your S3 bucket, publish to your SNS topic, and make `Describe` or `List` API requests to

get configuration details for your AWS resources. For more information about IAM roles, see IAM Roles in the *IAM User Guide*.

When you use the AWS Config console to create or update an IAM role, AWS Config automatically attaches the required permissions for you. For more information, see Setting Up AWS Config with the Console.

> **Policies and compliance results**
>
> IAM policies and other policies managed in AWS Organizations can impact whether AWS Config has permissions to record configuration changes for your resources. Additionally, rules directly evaluate the configuration of a resource and rules don't take into account these policies when running evaluations. Make sure that the policies in effect align with how you intend to use AWS Config.

**Contents**


- Creating IAM Role Policies
  - Adding an IAM Trust Policy to your Role
  - IAM Role Policy for your S3 Bucket
  - IAM Role Policy for KMS Key
  - IAM Role Policy for Amazon SNS Topic
  - IAM Role Policy for Getting Configuration Details
  - Managing Permissions for S3 Bucket Recording


## Creating IAM Role Policies

When you use the AWS Config console to create an IAM role, AWS Config automatically attaches the required permissions to the role for you.

If you are using the AWS CLI to set up AWS Config or you are updating an existing IAM role, you must manually update the policy to allow AWS Config to access your S3 bucket, publish to your SNS topic, and get configuration details about your resources.

### Adding an IAM Trust Policy to your Role

You can create an IAM trust policy that enables AWS Config to assume a role and use it to track your resources. For more information about trust policies, see Roles terms and concepts in the *IAM User Guide*.

The following is an example trust policy for AWS Config roles:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

You can use the `AWS:SourceAccount` condition in the IAM Role Trust relationship above to restrict the Config service principal to only interact with the AWS IAM Role when performing operations on behalf of specific accounts.

AWS Config also supports the `AWS:SourceArn` condition which restricts the Config service principal to only assume the IAM Role when performing operations on behalf of the owning account. When using the AWS Config service principal, the `AWS:SourceArn` property will always be set to `arn:aws:config:sourceRegion:sourceAccountID:*` where `sourceRegion` is the region of the customer managed configuration recorder and `sourceAccountID` is the ID of the account containing the customer managed configuration recorder.

For example, add the following condition restrict the Config service principal to only assume the IAM Role only on behalf of a customer managed configuration recorder in the `us-east-1` region in the account `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

### IAM Role Policy for your S3 Bucket

The following example policy grants AWS Config permission to access your S3 bucket:

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

### IAM Role Policy for KMS Key

The following example policy grants AWS Config permission to use KMS-based encryption on new objects for S3 bucket delivery:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
        }
    ]
}
```

### IAM Role Policy for Amazon SNS Topic

The following example policy grants AWS Config permission to access your SNS topic:

JSON

```
{
  "Version":"2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"arn:aws:sns:us-east-1:123456789012:MyTopic"
     }
    ]
}
```

If your SNS topic is encrypted for additional setup instructions, see Configuring AWS KMS Permissions in the *Amazon Simple Notification Service Developer Guide*.

**IAM Role Policy for Getting Configuration Details**

It is recommended to use the AWS Config service-linked role: `AWSServiceRoleForConfig`. Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services. The AWS Config service-linked role is required for service-linked configuration recorders. For more information, see Using Service-Linked Roles for AWS Config.

If you create or update a role with the console, AWS Config attaches the **AWSServiceRoleForConfig** for you.

If you use the AWS CLI, use the `attach-role-policy` command and specify the Amazon Resource Name (ARN) for **AWSServiceRoleForConfig**:

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForConfig
```

**Managing Permissions for S3 Bucket Recording**

AWS Config records and delivers notifications when an S3 bucket is created, updated, or deleted.

It is recommended to use the AWS Config service-linked role: `AWSServiceRoleForConfig`. Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services. The AWS Config service-linked role is required for service-linked configuration recorders. For more information, see Using Service-Linked Roles for AWS Config.

## Updating the IAM Role for the customer managed configuration recorder

You can update the IAM role used by the customer managed configuration recorder. Before you update the IAM role, ensure that you have created a new role to replace the old one. You must attach policies to the new role that grant permissions to AWS Config to record configurations and deliver them to your delivery channel.

For information about creating an IAM role and attaching the required policies to the IAM role, see Step 3: Creating an IAM Role.

> **Note**
>
> To find the ARN of an existing IAM role, go to the IAM console at https://console.aws.amazon.com/iam/. Choose **Roles** in the navigation pane. Then choose the name of the desired role and find the ARN at the top of the **Summary** page.

## Updating the IAM Role

You can update your IAM role using the AWS Management Console or the AWS CLI.

To update the IAM role (Console)

1. Sign in to the AWS Management Console and open the AWS Config console at https://console.aws.amazon.com/config/home.
2. Choose **Settings** in the navigation pane.
3. On the **Customer managed recorder** tab, choose **Edit** on the Settings page.
4. In the **Data governance**, section, choose the IAM role for AWS Config:
   - **Use an existing AWS Config service-linked role** – AWS Config creates a role that has the required permissions.
   - **Choose a role from your account** – For **Existing roles**, choose an IAM role in your account.
5. Choose **Save**.

To update the IAM role (AWS CLI)

Use the `put-configuration-recorder` command and specify the Amazon Resource Name (ARN) of the new role:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

# Permissions for the Amazon S3 Bucket for the AWS Config Delivery Channel

> **Important**
>
> This page is about setting up the Amazon S3 Bucket for the AWS Config delivery channel. This page is not about the `AWS::S3::Bucket` resource type that the AWS Config configuration recorder can record.

Amazon S3 buckets and objects are private by default. Only the AWS account that created the bucket (the resource owner) has access permissions. Resource owners can grant access to other resources and users by creating access policies.

When AWS Config automatically creates an S3 bucket for you, it adds the required permissions. However, if you specify an existing S3 bucket, you must add these permissions manually.

**Topics**


- Required Permissions for the Amazon S3 Bucket When Using IAM Roles
- Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles
- Granting AWS Config access to the Amazon S3 Bucket
- Required Permissions for the Amazon S3 Bucket When Delivering Cross-Account


## Required Permissions for the Amazon S3 Bucket When Using IAM Roles

AWS Config uses the IAM role you assigned to the configuration recorder to deliver configuration history and snapshots to S3 buckets in your account. For cross-account delivery, AWS Config first attempts to use the assigned IAM role. If the bucket policy doesn't grant `WRITE` access to the IAM role, AWS Config uses the `config.amazonaws.com` service principal. The bucket policy must grant `WRITE` access to `config.amazonaws.com` to complete the delivery. After successful delivery, AWS Config maintains ownership of all objects it delivers to the cross-account S3 bucket.

AWS Config calls the Amazon S3 HeadBucket API with the IAM role you assigned to the configuration recorder to confirm if the S3 bucket exists and its location. If you do not have the necessary permissions for AWS Config to confirm, you will see an `AccessDenied` error in your AWS CloudTrail logs. However, AWS Config can still deliver configuration history and snapshots

even if AWS Config does not have the necessary permissions to confirm if the S3 bucket exists and its location.

> **Minimum permissions**
>
> The Amazon S3 `HeadBucket` API requires the `s3:ListBucket` action.

## Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles

The AWS Config service-linked role does not have permission to put objects to Amazon S3 buckets. If you set up AWS Config using a service-linked role, AWS Config will use the `config.amazonaws.com` service principal to deliver configuration history and snapshots. The S3 bucket policy in your account or cross-account destinations must include permissions for the AWS Config service principal to write objects.

## Granting AWS Config access to the Amazon S3 Bucket

Complete the following steps enable AWS Config to deliver configuration history and snapshots to an Amazon S3 bucket.

1. Sign in to the AWS Management Console using the account that has the S3 bucket.
2. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
3. Select the bucket that you want AWS Config to use to deliver configuration items, and then choose **Properties**.
4. Choose **Permissions**.
5. Choose **Edit Bucket Policy**.
6. Copy the following policy into the **Bucket Policy Editor** window:

> **Security best practices**
>
> We strongly recommend that you restrict access in the bucket policy with the `AWS:SourceAccount` condition. This makes sure that AWS Config is granted access on behalf of expected users only.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
```

```
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

7. Substitute the following values in the bucket policy:

   - *amzn-s3-demo-bucket* – Name of the Amazon S3 bucket where AWS Config will deliver configuration history and snapshots.
   - *[optional] prefix* – An optional addition to the Amazon S3 object key that helps create a folder-like organization in the bucket.
   - *sourceAccountID* – ID of the account where AWS Config will deliver configuration history and snapshots.
8. Choose **Save** and then **Close**.

The `AWS:SourceAccount` condition restricts AWS Config operations to specified AWS accounts. For multi-account configurations within an organization delivering to a single S3 bucket, use IAM roles with AWS Organizations conditions keys instead of service-linked roles. For example, `AWS:PrincipalOrgID`. For more information, see Managing access permissions for an organization in the *AWS Organizations User guide*.

The `AWS:SourceArn` condition restricts AWS Config operations to specified delivery channels. The `AWS:SourceArn` format is as follows: `arn:aws:config:`*sourceRegion*`:`*123456789012*.

For example, to restrict S3 bucket access to a delivery channel in the US East (N. Virginia) Region for account 123456789012, add the following condition:

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

### Required Permissions for the Amazon S3 Bucket When Delivering Cross-Account

When AWS Config is configured to deliver configuration history and snapshots to an Amazon S3 bucket in a different account (cross-account setup), where the configuration recorder and the S3 bucket specified for delivery channel are in different AWS accounts, the following permissions are required:

- The IAM role you assign to the configuration recorder needs explicit permission to perform the `s3:ListBucket` operation. This is because AWS Config calls the Amazon S3 HeadBucket API with this IAM role to determine the bucket location.
- The S3 bucket policy must include permissions for the IAM role assigned to the configuration recorder.

The following is an example bucket policy configuration:

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
}
```

## Permissions for the KMS Key for the AWS Config Delivery Channel

Use the information in this topic if you want to create a policy for an AWS KMS key for your S3 bucket that allows you to use KMS-based encryption on objects delivered by AWS Config for S3 bucket delivery.

**Contents**


- Required Permissions for the KMS Key When Using IAM Roles (S3 Bucket Delivery)
- Required Permissions for the AWS KMS Key When Using Service-Linked Roles (S3 Bucket Delivery)
- Granting AWS Config access to the AWS KMS Key

## Required Permissions for the KMS Key When Using IAM Roles (S3 Bucket Delivery)

If you set up AWS Config using an IAM role, you can attach the follow permission policy to the KMS Key:

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> If the IAM role, Amazon S3 bucket policy, or AWS KMS key do not provide appropriate access to AWS Config, then AWS Config's attempt to send configuration information to the Amazon S3 bucket will fail. In this event, AWS Config sends the information again, this time as the AWS Config service principal. For this case, you must attach a permission policy, mentioned below, to the AWS KMS key to grant AWS Config access to use the key when delivering information to the Amazon S3 bucket.

## Required Permissions for the AWS KMS Key When Using Service-Linked Roles (S3 Bucket Delivery)

The AWS Config service-linked role does not have permission to access the AWS KMS key. So, if you set up AWS Config using a service-linked role, AWS Config will send information as the AWS Config service principal instead. You will need to attach an access policy, mentioned below, to the AWS KMS key to grant AWS Config access to use the AWS KMS key when delivering information to the Amazon S3 bucket.

### Granting AWS Config access to the AWS KMS Key

This policy allows AWS Config to use an AWS KMS key when delivering information to an Amazon S3 bucket

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Substitute the following values in the key policy:

- *myKMSKeyARN* – The ARN of the AWS KMS key used to encrypt data in the Amazon S3 bucket that AWS Config will deliver configuration items to.

- *sourceAccountID* – The ID of the account for which AWS Config will deliver configuration items to.

You can use the `AWS:SourceAccount` condition in the AWS KMS key policy above to restrict the Config service principal to only interact with the AWS KMS key when performing operations on behalf of specific accounts.

AWS Config also supports the `AWS:SourceArn` condition which restricts the Config service principal to only interact with the Amazon S3 bucket when performing operations on behalf of specific AWS Config delivery channels. When using the AWS Config service principal, the `AWS:SourceArn` property will always be set to `arn:aws:config:sourceRegion:sourceAccountID:*` where `sourceRegion` is the region of the delivery channel and `sourceAccountID` is the ID of the account containing the delivery channel. For more information on AWS Config delivery channels, see Managing the Delivery Channel. For example, add the following condition to restrict the Config service principal to interact with your Amazon S3 bucket only on behalf of a delivery channel in the `us-east-1` region in the account `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

## Permissions for the Amazon SNS Topic

> **Encrypted Amazon SNS not supported**
>
> AWS Config does not support encrypted Amazon SNS topics.

This topic describes how to configure AWS Config to deliver Amazon SNS topics owned by a different account. AWS Config must have the required permissions to send notifications to an Amazon SNS topic.

When the AWS Config console creates a new Amazon SNS topic for you, AWS Config grants the necessary permissions. If you choose an existing Amazon SNS topic, makes sure that the Amazon SNS topic includes the required permissions and follows security best practices.

**Cross-Region Amazon SNS topics are not supported**

AWS Config currently supports only access within the same AWS Region and across accounts.

**Contents**


- Required Permissions for the Amazon SNS Topic When Using IAM Roles
- Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles
- Granting AWS Config access to the Amazon SNS topic
- Troubleshooting for the Amazon SNS Topic


## Required Permissions for the Amazon SNS Topic When Using IAM Roles

You can attach a permissions policy to the Amazon SNS topic owned by a different account. If you want to use an Amazon SNS topic from another account, make sure to attach the following policy to the existing Amazon SNS topic.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

For the `Resource` key, *`account-id`* is the AWS account number of the topic owner. For *`account-id1`*, *`account-id2`*, and *`account-id3`*, use the AWS accounts that will send data to an Amazon SNS topic. You can substitute appropriate values for *`region`* and *`myTopic`*.

When AWS Config sends a notification to an Amazon SNS topic, it first attempts to use the IAM role, but this attempt fails if the role or AWS account does not have permission to publish to the topic. In this event, AWS Config sends the notification again, this time as an AWS Config service principal name (SPN). Before the publication can succeed, the access policy for the topic must grant `sns:Publish` access to the `config.amazonaws.com` principal name. You must attach an access policy, described in the next section, to the Amazon SNS topic to grant AWS Config access to the Amazon SNS topic if the IAM role does not have permission to publish to the topic.

## Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles

The AWS Config service-linked role does not have permission to access the Amazon SNS topic. So, if you set up AWS Config using a service-linked role (SLR), AWS Config will send information as the AWS Config service principal instead. You will need to attach an access policy, mentioned below, to the Amazon SNS topic to grant AWS Config access to send information to the Amazon SNS topic.

For same-account setup, when the Amazon SNS topic and SLR are in the same account and the Amazon SNS policy grants the SLR "`sns:Publish`" permission, you do not need to use the AWS Config SPN. The permissions policy below and security best practice recommendations are for cross-account setup.

## Granting AWS Config access to the Amazon SNS topic

This policy allows AWS Config to send a notification to an Amazon SNS topic. To grant AWS Config access to the Amazon SNS topic from another account, you will need to attach the following permissions policy.

> **Note**
>
> As a security best practice, it is strongly recommended to make sure AWS Config is accessing resources on behalf of expected users only by restricting access to the accounts listed in `AWS:SourceAccount` condition.

```
{
"Id": "Policy_ID",
```

```
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

For the `Resource` key, *`account-id`* is the AWS account number of the topic owner. For *`account-id1`*, *`account-id2`*, and *`account-id3`*, use the AWS accounts that will send data to an Amazon SNS topic. You can substitute appropriate values for *`region`* and *`myTopic`*.

You can use the `AWS:SourceAccount` condition in the previous Amazon SNS topic policy to restrict the AWS Config service principal name (SPN) to interact only with the Amazon SNS topic when performing operations on behalf of specific accounts.

AWS Config also supports the `AWS:SourceArn` condition which restricts the AWS Config service principal name (SPN) to only interact with the S3 bucket when performing operations on behalf of specific AWS Config delivery channels. When using the AWS Config service principal name (SPN), the `AWS:SourceArn` property will always be set to `arn:aws:config:sourceRegion:sourceAccountID:*` where `sourceRegion` is the Region of the delivery channel and `sourceAccountID` is the ID of the account containing the delivery channel. For more information about AWS Config delivery channels, see Managing the Delivery Channel. For example, add the following condition to restrict the AWS Config service principal name (SPN) to interact with your S3 bucket only on behalf of a delivery channel in the `us-east-1` Region in the account `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

### Troubleshooting for the Amazon SNS Topic

AWS Config must have permissions to send notifications to an Amazon SNS topic. If an Amazon SNS topic cannot receive notifications, verify that the IAM role that AWS Config was assuming has the required `sns:Publish` permissions.

## Troubleshooting AWS Config identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS Config and IAM.

**Topics**


- I am not authorized to perform an action in AWS Config
- I am not authorized to perform iam:PassRole
- I want to allow people outside of my AWS account to access my AWS Config resources


### I am not authorized to perform an action in AWS Config

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but does not have the fictional `config:`*`GetWidget`* permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

In this case, Mateo's policy must be updated to allow him to access the *`my-example-widget`* resource using the `config:`*`GetWidget`* action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

### I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to AWS Config.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in AWS Config. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

## I want to allow people outside of my AWS account to access my AWS Config resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether AWS Config supports these features, see How AWS Config works with IAM.
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

# Using Service-Linked Roles for AWS Config

AWS Config uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Config. Service-linked roles are predefined by AWS Config and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up AWS Config easier because you don't have to manually add the necessary permissions. AWS Config defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Config can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

## Service-Linked Role Permissions for AWS Config

AWS Config uses the service-linked role named **AwsServiceRoleForConfig** – AWS Config uses this service-linked role to call other AWS services on your behalf. To view the latest updates, see the section called "Policy updates".

The **AwsServiceRoleForConfig** service-linked role trusts the `config.amazonaws.com` service to assume the role.

The permissions policy for the `AwsServiceRoleForConfig` role contains read-only and write-only permissions for AWS Config resources and read-only permissions for resources in other services that AWS Config supports. To view the managed policy for **AwsServiceRoleForConfig**, see AWS managed policies for AWS Config.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

To use a service-linked role with AWS Config, you must configure permissions on your Amazon S3 bucket and Amazon SNS topic. For more information, see Required Permissions for the Amazon S3 Bucket When Using Service-Linked Roles, Required Permissions for the AWS KMS Key When Using Service-Linked Roles (S3 Bucket Delivery), and Required Permissions for the Amazon SNS Topic When Using Service-Linked Roles.

## Creating a Service-Linked Role for AWS Config

In the IAM CLI or the IAM API, create a service-linked role with the `config.amazonaws.com` service name. For more information, see Creating a Service-Linked Role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

## Editing a Service-Linked Role for AWS Config

AWS Config does not allow you to edit the **AwsServiceRoleForConfig** service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

## Deleting a Service-Linked Role for AWS Config

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

> **Note**
>
> If the AWS Config service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

### To delete AWS Config resources used by the AwsServiceRoleForConfig

Ensure that you do not have `ConfigurationRecorders` using the service-linked role. You can use the AWS Config console to stop the configuration recorder. To stop recording, under **Recording is on**, choose **Turn off**.

You can delete the `ConfigurationRecorder` using AWS Config API. To delete, use the `delete-configuration-recorder` command.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

**To manually delete the service-linked role using IAM**

Use the IAM console, the IAM CLI, or the IAM API to delete the AwsServiceRoleForConfig service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

# Incident Response in AWS Config

Security is the highest priority at AWS. As part of the AWS Cloud shared responsibility model, AWS manages a data center, network, and software architecture that meets the requirements of the most security-sensitive organizations. AWS is responsible for any incident response with respect to the AWS Config service itself. Also, as an AWS customer, you share a responsibility for maintaining security in the cloud. This means you control the security you choose to implement from the AWS tools and features you have access to, and are responsible for incident response on your side of the shared responsibility model.

By establishing a security baseline that meets the objectives for your applications running in the cloud, you're able to detect deviations that you can respond to. Since security incident response can be a complex topic, we encourage you to review the following resources so that you are better able to understand the impact that incident response (IR) and your choices have on your corporate goals: AWS Security Incident Response Guide, AWS Security Best Practices whitepaper, and the Security Perspective of the AWS Cloud Adoption Framework (CAF) white paper.

# Compliance Validation for AWS Config

Third-party auditors assess the security and compliance of AWS Config as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. For more information about your compliance responsibility when using AWS services, see AWS Security Documentation.

# Resilience in AWS Config

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

# Infrastructure Security in AWS Config

As a managed service, AWS Config is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access AWS Config through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

## Configuration and Vulnerability Analysis

For AWS Config, AWS handles basic security tasks such as guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

# Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service

can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions that AWS Config gives another service to the resource. Use `aws:SourceArn` if you want only one resource to be associated with the cross-service access. Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcard characters (*) for the unknown portions of the ARN. For example, `arn:aws:servicename:*:123456789012:*`.

If the `aws:SourceArn` value does not contain the account ID, such as an Amazon S3 bucket ARN, you must use both global condition context keys to limit permissions.

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in AWS Config to prevent the confused deputy problem: Granting AWS Config access to the Amazon S3 Bucket.

## Security Best Practices for AWS Config

AWS Config provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don’t represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

- Leverage tagging for AWS Config, which makes is easier to manage, search for, and filter resources.
- Confirm your delivery channels have been properly set, and once confirmed, verify that AWS Config is recording properly.

For more information, see AWS Config best practices blog.

# Logging and Monitoring in AWS Config

AWS Config is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Config. Monitoring is an important part of maintaining the reliability, availability, and performance of AWS Config and your AWS solutions.

**Topics**


- Logging AWS Config API Calls with AWS CloudTrail
- Monitoring


## Logging AWS Config API Calls with AWS CloudTrail

CloudTrail captures all API calls for AWS Config as events. The calls captured include calls from the AWS Config console and code calls to the AWS Config API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Config. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Config, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

**Topics**


- AWS Config Information in CloudTrail
- Understanding AWS Config Log File Entries
- Example Log Files


### AWS Config Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS Config, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for AWS Config, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you

create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All AWS Config operations are logged by CloudTrail and are documented in the AWS Config API Reference. For example, calls to the DeliverConfigSnapshot, DeleteDeliveryChannel, and DescribeDeliveryChannels operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

## Understanding AWS Config Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

## Example Log Files

For examples of the CloudTrail log entries, see the following topics.

## DeleteDeliveryChannel

The following is an example CloudTrail log file for the DeleteDeliveryChannel operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## DeliverConfigSnapshot

The following is an example CloudTrail log file for the DeliverConfigSnapshot operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
```

```
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

## DescribeConfigurationRecorderStatus

The following is an example CloudTrail log file for the DescribeConfigurationRecorderStatus operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
```

```
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## DescribeConfigurationRecorders

The following is an example CloudTrail log file for the DescribeConfigurationRecorders operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
```

```
      "recipientAccountId": "222222222222"
    }
```

## DescribeDeliveryChannels

Following is an example CloudTrail log file for the DescribeDeliveryChannels operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## GetResourceConfigHistory

The following is an example CloudTrail log file for the GetResourceConfigHistory operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

## PutConfigurationRecorder

The following is an example CloudTrail log file for the PutConfigurationRecorder operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
```

```
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## PutDeliveryChannel

The following is an example CloudTrail log file for the PutDeliveryChannel operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
```

```
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

## StartConfigurationRecorder

The following is an example CloudTrail log file for the StartConfigurationRecorder operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

The following is an example CloudTrail log file for the StopConfigurationRecorder operation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

# Monitoring

You can use other AWS services to monitor AWS Config resources.

- You can use Amazon Simple Notification Service (SNS) to send you notifications every time a supported AWS resource is created, updated, or otherwise modified as a result of user API activity.
- You can use Amazon EventBridge to detect and react to changes in the status of AWS Config events.

**Topics**


- Monitoring AWS Resource Changes with Amazon SQS
- Monitoring AWS Config with Amazon EventBridge


## Monitoring AWS Resource Changes with Amazon SQS

AWS Config uses Amazon Simple Notification Service (SNS) to send you notifications every time a supported AWS resource is created, updated, or otherwise modified as a result of user API activity. However, you might be interested in only certain resource configuration changes. For example, you might consider it critical to know when someone modifies the configuration of a security group, but not need to know every time there is a change to tags on your Amazon EC2 instances. Or, you might want to write a program that performs specific actions when specific resources are updated. For example, you might want to start a certain workflow when a security group configuration is changed. If you want to programmatically consume the data from AWS Config in these or other ways, use an Amazon Simple Queue Service queue as the notification endpoint for Amazon SNS.

> **Note**
>
> Notifications can also come from Amazon SNS in the form of an email, a Short Message Service (SMS) message to SMS-enabled mobile phones and smartphones, a notification message to an application on a mobile device, or a notification message to one or more HTTP or HTTPS endpoints.

You can have a single SQS queue subscribe to multiple topics, whether you have one topic for each region or one topic for each account for each region. You must subscribe the queue to your desired SNS topic. (You can subscribe multiple queues to one SNS topic.) For more information, see Sending Amazon SNS Messages to Amazon SQS Queues.

### Permissions for Amazon SQS

To use Amazon SQS with AWS Config, you must configure a policy that grants permissions to your account to perform all actions that are allowed on an SQS queue. The following example policy grants the account number 111122223333 and account number 444455556666 permission to send messages pertaining to each configuration change to the queue named arn:aws:sqs:us-east-2:444455556666:queue1.

JSON

```
{
  "Version":"2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

You must also create a policy that grants permissions for connections between an SNS topic and the SQS queue that subscribes to that topic. The following is an example policy that permits the SNS topic with the Amazon Resource Name (ARN) arn:aws:sns:us-east-2:111122223333:test-topic to perform any actions on the queue named arn:aws:sqs:us-east-2:111122223333:test-topic-queue.

> **Note**
>
> The account for the SNS topic and the SQS queue must be in the same region.

JSON

```
{
  "Version":"2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Each policy can include statements that cover only a single queue, not multiple queues. For information about other restrictions on Amazon SQS policies, see Special Information for Amazon SQS Policies.

## Monitoring AWS Config with Amazon EventBridge

Amazon EventBridge delivers a near real-time stream of system events that describe changes in AWS resources. Use Amazon EventBridge to detect and react to changes in the status of AWS Config events.

You can create a rule that runs whenever there is a state transition, or when there is a transition to one or more states that are of interest. Then, based on rules you create, Amazon EventBridge invokes one or more target actions when an event matches the values you specify in a rule. Depending on the type of event, you might want to send notifications, capture event information, take corrective action, initiate events, or take other actions.

Before you create event rules for AWS Config, however, you should do the following:

- Familiarize yourself with events, rules, and targets in EventBridge. For more information, see What Is Amazon EventBridge?
- For more information about how to get started with EventBridge and set up rules, see Getting started with Amazon EventBridge.
- Create the target or targets you will use in your event rules.

### Topics

- Considerations

- Amazon EventBridge format for AWS Config
- Creating Amazon EventBridge Rule for AWS Config

## Considerations

You will not receive alerts through EventBridge for the following resource types if you are not recording them with AWS Config:

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`
- `AWS::EC2::Host`
- `AWS::EC2::Instance`
- `AWS::EC2::InternetGateway`
- `AWS::EC2::NetworkAcl`
- `AWS::EC2::NetworkInterface`
- `AWS::EC2::RouteTable`
- `AWS::EC2::SecurityGroup`
- `AWS::EC2::Subnet`
- `AWS::EC2::VPC`
- `AWS::EC2::VPNConnection`
- `AWS::EC2::VPNGateway`
- `AWS::EC2::Volume`
- `AWS::ElasticLoadBalancingV2::LoadBalancer`
- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`
- `AWS::RDS::DBInstance`
- `AWS::RDS::DBSecurityGroup`

- AWS::RDS::DBSnapshot
- AWS::RDS::DBSubnetGroup
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

## Amazon EventBridge format for AWS Config

The EventBridge event for AWS Config has the following format:

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

## Creating Amazon EventBridge Rule for AWS Config

Use the following steps to create an EventBridge rule that triggers on an event emitted by AWS Config. Events are emitted on a best effort basis.

1. In the navigation pane, choose **Rules**.
2. Choose **Create rule**.
3. Enter a name and description for the rule.

   A rule can't have the same name as another rule in the same Region and on the same event bus.

   > **Note**
   >
   > An event bus receives events from a source, uses rules to evaluate them, applies any configured input transformation, and routes them to the appropriate target(s). Your account's default event bus receives events from AWS services. A custom event bus can receive events from your custom applications and services. A partner event bus receives events from an event source created by an SaaS partner. These events come from the partners services or applications. For more information, see Event buses in Amazon EventBridge in the *Amazon EventBridge User Guide*.

4. For **Rule type**, choose **Rule with an event pattern**.
5. For **Event source**, choose **AWS events or EventBridge partner events**.
6. (Optional) For **Sample event type**, choose **AWS events**.
7. (Optional) For **Sample events**, choose the event type that triggers the rule:
   - Choose **AWS API Call from CloudTrail** to base rules on API calls made to this service. For more information about creating this type of rule, see Tutorial: Create an Amazon EventBridge rule for AWS CloudTrail API calls.
   - Choose **Config Configuration Item Change** to get notifications when a resource in your account changes.

     As described in these support articles, you can use EventBridge to receive custom email notifications when a resource is created or deleted, How can I receive custom email notifications when a resource is created in my AWS account using AWS Config service? and How can I receive custom email notifications when a resource is deleted in my AWS account using AWS Config service?.
   - Choose **Config Rules Compliance Change** to get notifications when a compliance check to your rules fails.

As described in this support article, you can use EventBridge to receive custom email notifications when a resource is noncompliant, How can I be notified when an AWS resource is noncompliant using AWS Config?.

- Choose **Config Rules Re-evaluation Status** to get reevaluation status notifications.
- Choose **Config Configuration Snapshot Delivery Status** to get configuration snapshot delivery status notifications.
- Choose **Config Configuration History Delivery Status** to get configuration history delivery status notifications.

8. For **Creation method**, choose **Use pattern form**.
9. For **Event source**, choose **AWS services**.
10. For **AWS service**, choose **Config**.
11. For **Event type**, choose the event type that triggers the rule:

- Choose **All Events** to make a rule that applies to all AWS services. If you choose this option, you cannot choose specific message types, rule names, resource types, or resource IDs.
- Choose **AWS API Call from CloudTrail** to base rules on API calls made to this service. For more information about creating this type of rule, see Tutorial: Create an Amazon EventBridge rule for AWS CloudTrail API calls.
- Choose **Config Configuration Item Change** to get notifications when a resource in your account changes.

  As described in these support articles, you can use EventBridge to receive custom email notifications when a resource is created or deleted, How can I receive custom email notifications when a resource is created in my AWS account using AWS Config service? and How can I receive custom email notifications when a resource is deleted in my AWS account using AWS Config service?.
- Choose **Config Rules Compliance Change** to get notifications when a compliance check to your rules fails.

  As described in this support article, you can use EventBridge to receive custom email notifications when a resource is noncompliant, How can I be notified when an AWS resource is noncompliant using AWS Config?.
- Choose **Config Rules Re-evaluation Status** to get reevaluation status notifications.
- Choose **Config Configuration Snapshot Delivery Status** to get configuration snapshot delivery status notifications.

- Choose **Config Configuration History Delivery Status** to get configuration history delivery status notifications.

12. Choose **Any message type** to receive notifications of any type. Choose **Specific message type(s)** to receive the following types of notifications:
    - If you choose **ConfigurationItemChangeNotification**, you receive messages when the configuration of a resource that AWS Config evaluates has changed.
    - If you choose **ComplianceChangeNotification**, you receive messages when the compliance type of a resource that AWS Config evaluates has changed.
    - If you choose **ConfigRulesEvaluationStarted**, you receive messages when AWS Config starts evaluating your rule against the specified resources.
    - If you choose **ConfigurationSnapshotDeliveryCompleted**, you receive messages when AWS Config successfully delivers the configuration snapshot to your Amazon S3 bucket.
    - If you choose **ConfigurationSnapshotDeliveryFailed**, you receive messages when AWS Config fails to deliver the configuration snapshot to your Amazon S3 bucket.
    - If you choose **ConfigurationSnapshotDeliveryStarted**, you receive messages when AWS Config starts delivering the configuration snapshot to your Amazon S3 bucket.
    - If you choose **ConfigurationHistoryDeliveryCompleted**, you receive messages when AWS Config successfully delivers the configuration history to your Amazon S3 bucket.
13. If you chose a specific event type from the **Event Type** dropdown list, choose **Any resource type** to make a rule that applies to all AWS Config supported resource types.

    Or choose **Specific resource type(s)**, and then type the AWS Config supported resource type (for example, `AWS::EC2::Instance`).
14. If you chose a specific event type from the **Event Type** dropdown list, choose **Any resource ID** to include any AWS Config supported resource ID.

    Or choose **Specific resource ID(s)**, and then type the AWS Config supported resource ID (for example, `i-04606de676e635647`).
15. If you chose a specific event type from the **Event Type** dropdown list, choose **Any rule name** to include any AWS Config supported rule.

    Or choose **Specific rule name(s)**, and then type the AWS Config supported rule (for example, **required-tags**).
16. For **Select target(s)**, choose the type of target you have prepared to use with this rule, and then configure any additional options required by that type.

17. The fields displayed vary depending on the service you choose. Enter information specific to this target type as needed.
18. For many target types, EventBridge needs permissions to send events to the target. In these cases, EventBridge can create the IAM role needed for your rule to run.
    - To create an IAM role automatically, choose **Create a new role for this specific resource**.
    - To use an IAM role that you created earlier, choose **Use existing role**.
19. (Optional) Choose **Add target** to add another target for this rule.
20. (Optional) Enter one or more tags for the rule. For more information, see Amazon EventBridge tags.
21. Review your rule setup to make sure it meets your event-monitoring requirements.
22. Choose **Create** to confirm your selection.

# Using AWS Config with Interface Amazon VPC Endpoints

If you use Amazon Virtual Private Cloud (Amazon VPC) to host your AWS resources, you can establish a private connection between your VPC and AWS Config. You can use this connection to communicate with AWS Config from your VPC without going through the public internet.

Amazon VPC is an AWS service that you can use to launch AWS resources in a virtual network that you define. With a VPC, you have control over your network settings, such the IP address range, subnets, route tables, and network gateways. Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IP addresses. To connect your VPC to AWS Config, you define an *interface VPC endpoint* for AWS Config. This type of endpoint enables you to connect your VPC to AWS services. The endpoint provides reliable, scalable connectivity to AWS Config without requiring an internet gateway, network address translation (NAT) instance, or VPN connection. For more information, see What is Amazon VPC in the *Amazon VPC User Guide*.

The following steps are for users of Amazon VPC. For more information, see Getting Started in the *Amazon VPC User Guide*.

## Create a VPC Endpoint for AWS Config

To start using AWS Config with your VPC, create an interface VPC endpoint for AWS Config. You do not need to change the settings for AWS Config. AWS Config calls other AWS services using their public endpoints. For more information, see Creating an Interface Endpoint in the *Amazon VPC User Guide*.

# Frequently Asked Questions

## Unable to see my latest configuration changes

### Can I expect to view my configuration changes right away?

AWS Config usually records configuration changes to your resources right after a change is detected, or at the frequency that you specify. However, this is on a best effort basis and can take longer at times. If issues persist after sometime, contact Support and provide your AWS Config metrics that are supported by Amazon CloudWatch. For information about these metrics, see AWS Config Usage and Success Metrics.

## Indirect Relationships in AWS Config

**Topics**


- What is resource relationship?
- What is a direct and an indirect relationship with respect to a resource?
- Which indirect relationships does AWS Config support?
- Which scenarios uses indirect relationship?
- How are the configuration items created due to direct and indirect relationship?
- What are the configuration items generated due to indirect relationships?
- How do I disable indirect relationship?
- How do I retrieve configuration data related to indirect relationships?


### What is resource relationship?

In AWS, resources refer to entities that are manageable, such as an Amazon Elastic Compute Cloud (Amazon EC2) instance, an AWS CloudFormation stack, or an Amazon S3 bucket. AWS Config is a service that tracks and monitors resources by creating configuration items (CIs) whenever a change to a recorded resource type is detected, or at the recording frequency that you set. For instance, when AWS Config is set up to track Amazon EC2 instances, it creates a configuration item every time an instance is created, updated, or deleted. Each configuration item created by AWS Config has several fields, including `accountId`, `arn` (Amazon Resource Name), `awsRegion`, `configuration`, `tags`, and `relationships`. The relationships field of a CI enables AWS Config

to display how resources are linked to one another. For instance, a relationship may indicate that an Amazon EBS volume with ID `vol-123ab45d` is attached to an Amazon EC2 instance with ID `i-a1b2c3d4`, which is associated with security group `sg-ef678hk`.

## What is a direct and an indirect relationship with respect to a resource?

AWS Config derives the relationships for most resource types from the configuration field, which are called "direct" relationships. A direct relationship is a one-way connection (A→B) between a resource (A) and another resource (B), typically obtained from the describe API response of resource (A). In the past, for some resource types that AWS Config initially supported, it also captured relationships from the configurations of other resources, creating "indirect" relationships that are bidirectional (B→A). For example, the relationship between an Amazon EC2 instance and its security group is direct because the security groups are included in the describe API response for the Amazon EC2 instance. On the other hand, the relationship between a security group and an Amazon EC2 instance is indirect because describing a security group does not return any information about the instances it is associated with.

For example, indirect relationships can help answer the following questions:

- When a NAT Gateway fails, which EC2 instances in private subnets are affected?
- If a route table is modified, which EC2 instance might experience connectivity issues?
- Which security group was never used?
- Which secondary ENI attached to an EC2 instance is associated with the security group?

As a result, when a resource configuration change is detected, AWS Config not only creates a CI for that resource, but also generates CIs for any related resources, including those with indirect relationships. For example, when AWS Config detects changes in an Amazon EC2 instance, it creates a CI for the instance and a CI for the security group that is associated with the instance.

## Which indirect relationships does AWS Config support?

The following indirect resource relationships are supported in AWS Config.

| Resource type | is indirectly related to the resource type | | |
|---|---|---|---|
| `AWS::EC2::RouteTable` | `AWS::EC2::Instance` | | |

| Resource type | is indirectly related to the resource type | | |
|---|---|---|---|
| | , AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , AWS::EC2::VPC | | |
| AWS::EC2::EIP | AWS::EC2::Instance , AWS::EC2::NetworkInterface | | |
| AWS::EC2::Instance | AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC | | |
| AWS::EC2::NetworkInterface | AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC | | |
| AWS::EC2::NetworkACL | AWS::EC2::Subnet , AWS::EC2::VPC | | |

| Resource type | is indirectly related to the resource type | | |
|---|---|---|---|
| AWS::EC2::VPNConnection | AWS::EC2::VPNGateway ,AWS::EC2::CustomerGateway | | |
| AWS::EC2::InternetGateway | AWS::EC2::VPC | | |
| AWS::EC2::SecurityGroup | AWS::EC2::VPC | | |
| AWS::EC2::Subnet | AWS::EC2::VPC | | |
| AWS::EC2::VPNGateway | AWS::EC2::VPC | | |

## Which scenarios uses indirect relationship?

Below are the AWS services and the service's feature using indirect relationship.

| AWS feature | Scenario |
|---|---|
| AWS Config managed rule | ec2-security-group-attached-to-eni rule checks whether non-default security groups are attached to Elastic Network Interfaces (ENI).<br><br>Without an indirect relationship, you would need to create a custom rule to check if non-default security groups are attached to an ENI. |

| AWS feature | Scenario |
| --- | --- |
| AWS Firewall Manager | Usage Audit Security Group policy uses indirect relationship to understand when a security group was last used.<br><br>Without an indirect relationship, you would need to build and associate a security group to new resources at the same time to avoid triggering the rule with AWS Firewall Manager. |
| Default resources | • Default resources when a non-default VPC is created:<br>  • Default security group, default network ACL, and default route table.<br>• Default resources when a default VPC is created:<br>  • Everything that is created with non-defau lt VPC, an internet gateway, and default subnet in each Availability Zone that you have access to.<br>• Default VPC creation itself when an account calls EC2 for first time ever.<br>  • Default subnet created for accounts in a newly launched Availability Zone.<br><br>Without an indirect relationship, you would need to wait up to 12 hours for automatic baselining to record changes to default resources. |

## How are the configuration items created due to direct and indirect relationship?

For a direct relationship between resources (A→B), any configuration change to the resource B will initiate a configuration item (CI) for the resource A as well. Similarly, for an indirect relationship (B→A), when there is a configuration change to resource A a new CI will be generated for resource B. For example, Amazon EC2 instance to security group is a direct relationship so any configuration change to a security group would generate a CI for the security group as well as a CI for the EC2 instance. Similarly, security group to Amazon EC2 instance is an indirect relationship so any configuration change to an EC2 instance would generate a CI for the Amazon EC2 instance as well as a CI for the security group.

## What are the configuration items generated due to indirect relationships?

Below are the additional configuration items (CIs) generated due to indirect resource relationships.

| Configuration changes to the following resource types | will generate CIs for the following resources types | | |
|---|---|---|---|
| `AWS::EC2::RouteTable` | `AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` , `AWS::EC2::VPNGateway` , and `AWS::EC2::VPC` | | |
| `AWS::EC2::EIP` | `AWS::EC2::Instance` , `AWS::EC2:` | | |

| Configuration changes to the following resource types | will generate CIs for the following resources types | | |
|---|---|---|---|
| | :NetworkInterface | | |
| AWS::EC2::Instance | AWS::EC2::Security Group ,AWS::EC2::Subnet , AWS::EC2::VPC | | |
| AWS::EC2::NetworkInterface | AWS::EC2::Security Group , AWS::EC2::Subnet , AWS::EC2::VPC | | |
| AWS::EC2::NetworkACL | AWS::EC2::Subnet , AWS::EC2::VPC | | |
| AWS::EC2::VPNConnection | AWS::EC2::VPNGateway ,AWS::EC2::Customer Gateway | | |
| AWS::EC2::Internet Gateway | AWS::EC2::VPC | | |
| AWS::EC2::SecurityGroup | AWS::EC2::VPC | | |

| Configuration changes to the following resource types | will generate CIs for the following resources types | | |
|---|---|---|---|
| `AWS::EC2::Subnet` | `AWS::EC2::VPC` | | |
| `AWS::EC2::VPNGateway` | `AWS::EC2::VPC` | | |

## How do I disable indirect relationship?

Complete the following steps to disable indirect relationship:

1. Open an AWS Support case from your account or from the management account for multiple accounts.
2. Select **Technical** for the support type.
3. For Service, select **AWS Config**.
4. For Category, select **Other**.
5. Select appropriate severity level.
6. Enter **Disable Indirect Relationship** in the subject line.
7. In the description:
   - Confirm you have read this FAQ and want to proceed.
   - List the regions where you want to disable indirect relationship.
   - If submitting from a management account, include account IDs and their associated regions.
   - For multiple accounts, you may attach a CSV file with account IDs and regions.

An AWS Support engineer will provide next steps and status updates. We recommend that you maintain a list of AWS accounts and regions where indirect relationship is disabled. For new accounts, submit a new AWS Support case to disable indirect relationship.

## How do I retrieve configuration data related to indirect relationships?

You can run Structured Query Language (SQL) queries in AWS Config Advanced Queries to retrieve configuration data related to indirect resource relationships. For example, if you want to retrieve the list of Amazon EC2 instances related to a security group, use the following query:

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

# Code examples for AWS Config using AWS SDKs

The following code examples show how to use AWS Config with an AWS software development kit (SDK).

*Actions* are code excerpts from larger programs and must be run in context. While actions show you how to call individual service functions, you can see actions in context in their related scenarios.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

**Code examples**


- Basic examples for AWS Config using AWS SDKs
  - Actions for AWS Config using AWS SDKs
    - Use DeleteConfigRule with an AWS SDK or CLI
    - Use DescribeComplianceByConfigRule with a CLI
    - Use DescribeComplianceByResource with a CLI
    - Use DescribeConfigRuleEvaluationStatus with a CLI
    - Use DescribeConfigRules with an AWS SDK or CLI
    - Use DescribeConfigurationRecorderStatus with a CLI
    - Use DescribeConfigurationRecorders with a CLI
    - Use DescribeDeliveryChannels with a CLI
    - Use GetComplianceDetailsByConfigRule with a CLI
    - Use GetComplianceDetailsByResource with a CLI
    - Use GetComplianceSummaryByConfigRule with a CLI
    - Use GetComplianceSummaryByResourceType with a CLI
    - Use PutConfigRule with an AWS SDK or CLI
    - Use PutDeliveryChannel with a CLI


## Basic examples for AWS Config using AWS SDKs

The following code examples show how to use the basics of AWS Config with AWS SDKs.

**Examples**

- Actions for AWS Config using AWS SDKs
  - Use DeleteConfigRule with an AWS SDK or CLI
  - Use DescribeComplianceByConfigRule with a CLI
  - Use DescribeComplianceByResource with a CLI
  - Use DescribeConfigRuleEvaluationStatus with a CLI
  - Use DescribeConfigRules with an AWS SDK or CLI
  - Use DescribeConfigurationRecorderStatus with a CLI
  - Use DescribeConfigurationRecorders with a CLI
  - Use DescribeDeliveryChannels with a CLI
  - Use GetComplianceDetailsByConfigRule with a CLI
  - Use GetComplianceDetailsByResource with a CLI
  - Use GetComplianceSummaryByConfigRule with a CLI
  - Use GetComplianceSummaryByResourceType with a CLI
  - Use PutConfigRule with an AWS SDK or CLI
  - Use PutDeliveryChannel with a CLI

## Actions for AWS Config using AWS SDKs

The following code examples demonstrate how to perform individual AWS Config actions with AWS SDKs. Each example includes a link to GitHub, where you can find instructions for setting up and running the code.

The following examples include only the most commonly used actions. For a complete list, see the AWS Config API Reference.

**Examples**

- Use DeleteConfigRule with an AWS SDK or CLI
- Use DescribeComplianceByConfigRule with a CLI
- Use DescribeComplianceByResource with a CLI
- Use DescribeConfigRuleEvaluationStatus with a CLI
- Use DescribeConfigRules with an AWS SDK or CLI
- Use DescribeConfigurationRecorderStatus with a CLI

- Use DescribeConfigurationRecorders with a CLI
- Use DescribeDeliveryChannels with a CLI
- Use GetComplianceDetailsByConfigRule with a CLI
- Use GetComplianceDetailsByResource with a CLI
- Use GetComplianceSummaryByConfigRule with a CLI
- Use GetComplianceSummaryByResourceType with a CLI
- Use PutConfigRule with an AWS SDK or CLI
- Use PutDeliveryChannel with a CLI

## Use `DeleteConfigRule` with an AWS SDK or CLI

The following code examples show how to use `DeleteConfigRule`.

CLI

**AWS CLI**

**To delete an AWS Config rule**

The following command deletes an AWS Config rule named `MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- For API details, see DeleteConfigRule in *AWS CLI Command Reference*.

Python

**SDK for Python (Boto3)**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class ConfigWrapper:
```

```
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- For API details, see DeleteConfigRule in *AWS SDK for Python (Boto3) API Reference*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `DescribeComplianceByConfigRule` with a CLI

The following code examples show how to use `DescribeComplianceByConfigRule`.

CLI

**AWS CLI**

**To get compliance information for your AWS Config rules**

The following command returns compliance information for each AWS Config rule that is violated by one or more AWS resources:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many resources do not comply with the related rule. For example, the following output indicates that 3 resources do not comply with the rule named `InstanceTypesAreT2micro`.

Output:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- For API details, see DescribeComplianceByConfigRule in *AWS CLI Command Reference*.

PowerShell

### Tools for PowerShell V4

#### Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

**Output:**

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

#### Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

### Tools for PowerShell V5

#### Example 1: This example retrieves compliances details for the rule ebs-optimized-instance, for which there is no current evaluation results for the rule, hence it returns INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

**Output:**

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

**Example 2: This example returns the number of non-compliant resources for the rule ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.**

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       2
```

- For API details, see DescribeComplianceByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `DescribeComplianceByResource` with a CLI

The following code examples show how to use `DescribeComplianceByResource`.

CLI

**AWS CLI**

**To get compliance information for your AWS resources**

The following command returns compliance information for each EC2 instance that is recorded by AWS Config and that violates one or more rules:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

In the output, the value for each `CappedCount` attribute indicates how many rules the resource violates. For example, the following output indicates that instance `i-1a2b3c4d` violates 2 rules.

Output:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- For API details, see DescribeComplianceByResource in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.**

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

**Output:**

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example checks the `AWS::SSM::ManagedInstanceInventory` resource type for 'COMPLIANT' compliance type.**

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

**Output:**

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- For API details, see DescribeComplianceByResource in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `DescribeConfigRuleEvaluationStatus` with a CLI

The following code examples show how to use `DescribeConfigRuleEvaluationStatus`.

CLI

### AWS CLI

#### To get status information for an AWS Config rule

The following command returns the status information for an AWS Config rule named `MyConfigRule`:

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

Output:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- For API details, see DescribeConfigRuleEvaluationStatus in *AWS CLI Command Reference*.

PowerShell

### Tools for PowerShell V4

#### Example 1: This sample returns the status information for the given config rules.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

**Output:**

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- For API details, see DescribeConfigRuleEvaluationStatus in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

## Tools for PowerShell V5

### Example 1: This sample returns the status information for the given config rules.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

**Output:**

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
```

```
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- For API details, see DescribeConfigRuleEvaluationStatus in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `DescribeConfigRules` with an AWS SDK or CLI

The following code examples show how to use `DescribeConfigRules`.

CLI

### AWS CLI

#### To get details for an AWS Config rule

The following command returns details for an AWS Config rule named `InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Output:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- For API details, see DescribeConfigRules in *AWS CLI Command Reference*.

PowerShell

### Tools for PowerShell V4

#### Example 1: This sample lists config rules for the account, with selected properties.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

#### Output:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

### Tools for PowerShell V5

#### Example 1: This sample lists config rules for the account, with selected properties.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

#### Output:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
```

```
--------------                                    ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                             config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                               config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required        config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- For API details, see DescribeConfigRules in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

## Python

### SDK for Python (Boto3)

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.
```

```
        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- For API details, see DescribeConfigRules in *AWS SDK for Python (Boto3) API Reference*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `DescribeConfigurationRecorderStatus` with a CLI

The following code examples show how to use `DescribeConfigurationRecorderStatus`.

CLI

### AWS CLI

#### To get status information for the configuration recorder

The following command returns the status of the default configuration recorder:

```
aws configservice describe-configuration-recorder-status
```

Output:

```
{
```

```
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- For API details, see DescribeConfigurationRecorderStatus in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This sample returns status of the configuration recorders.**

```
Get-CFGConfigurationRecorderStatus
```

**Output:**

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- For API details, see DescribeConfigurationRecorderStatus in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This sample returns status of the configuration recorders.**

```
Get-CFGConfigurationRecorderStatus
```

**Output:**

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- For API details, see DescribeConfigurationRecorderStatus in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `DescribeConfigurationRecorders` with a CLI

The following code examples show how to use `DescribeConfigurationRecorders`.

CLI

### AWS CLI

**To get details about the configuration recorder**

The following command returns details about the default configuration recorder:

```
aws configservice describe-configuration-recorders
```

Output:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
```

```
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- For API details, see DescribeConfigurationRecorders in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example returns the details of configuration recorders.**

```
Get-CFGConfigurationRecorder | Format-List
```

**Output:**

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- For API details, see DescribeConfigurationRecorders in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example returns the details of configuration recorders.**

```
Get-CFGConfigurationRecorder | Format-List
```

**Output:**

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- For API details, see DescribeConfigurationRecorders in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `DescribeDeliveryChannels` with a CLI

The following code examples show how to use `DescribeDeliveryChannels`.

CLI

**AWS CLI**

**To get details about the delivery channel**

The following command returns details about the delivery channel:

```
aws configservice describe-delivery-channels
```

Output:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- For API details, see DescribeDeliveryChannels in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example retrieves the delivery channel for the region and displays details.**

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

**Output:**

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example retrieves the delivery channel for the region and displays details.**

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

**Output:**

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- For API details, see DescribeDeliveryChannels in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `GetComplianceDetailsByConfigRule` with a CLI

The following code examples show how to use `GetComplianceDetailsByConfigRule`.

CLI

## AWS CLI

### To get the evaluation results for an AWS Config rule

The following command returns the evaluation results for all of the resources that don't comply with an AWS Config rule named `InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- For API details, see GetComplianceDetailsByConfigRule in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

**Output:**

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

**Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

**Output:**

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example obtains the evaluation results for the rule access-keys-rotated and returns the output grouped by compliance-type**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

**Output:**

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

**Example 2: This example queries compliance details for the rule access-keys-rotated for COMPLIANT resources.**

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

**Output:**

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- For API details, see GetComplianceDetailsByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `GetComplianceDetailsByResource` with a CLI

The following code examples show how to use `GetComplianceDetailsByResource`.

CLI

### AWS CLI

#### To get the evaluation results for an AWS resource

The following command returns the evaluation results for each rule with which the EC2 instance `i-1a2b3c4d` does not comply:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Output:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
```

```
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- For API details, see GetComplianceDetailsByResource in *AWS CLI Command Reference*.

PowerShell

### Tools for PowerShell V4

#### Example 1: This example evaulation results for the given resource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

#### Output:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- For API details, see GetComplianceDetailsByResource in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example evaulation results for the given resource.**

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

**Output:**

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- For API details, see GetComplianceDetailsByResource in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `GetComplianceSummaryByConfigRule` with a CLI

The following code examples show how to use `GetComplianceSummaryByConfigRule`.

CLI

**AWS CLI**

**To get the compliance summary for your AWS Config rules**

The following command returns the number of rules that are compliant and the number that are noncompliant:

```
aws configservice get-compliance-summary-by-config-rule
```

In the output, the value for each CappedCount attribute indicates how many rules are compliant or noncompliant.

Output:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- For API details, see GetComplianceSummaryByConfigRule in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This sample returns the number of Config rules that are non-compliant.**

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This sample returns the number of Config rules that are non-compliant.**

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

**Output:**

```
CapExceeded CappedCount
----------- -----------
False       9
```

- For API details, see GetComplianceSummaryByConfigRule in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `GetComplianceSummaryByResourceType` with a CLI

The following code examples show how to use `GetComplianceSummaryByResourceType`.

CLI

**AWS CLI**

**To get the compliance summary for all resource types**

The following command returns the number of AWS resources that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type
```

In the output, the value for each `CappedCount` attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
```

```
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

**To get the compliance summary for a specific resource type**

The following command returns the number of EC2 instances that are noncompliant and the number that are compliant:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

In the output, the value for each `CappedCount` attribute indicates how many resources are compliant or noncompliant.

Output:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
```

```
        }
    ]
}
```

- For API details, see GetComplianceSummaryByResourceType in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.**

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This sample returns the number of resources that are compliant or noncompliant and converts the output to json.**

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
```

```
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- For API details, see GetComplianceSummaryByResourceType in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `PutConfigRule` with an AWS SDK or CLI

The following code examples show how to use `PutConfigRule`.

CLI

**AWS CLI**

**To add an AWS managed Config rule**

The following command provides JSON code to add an AWS managed Config rule:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
```

```
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so AWS Config will evaluate only EC2 instances against the rule. Because the rule is a managed rule, the `Owner` attribute is set to `AWS`, and the `SourceIdentifier` attribute is set to the rule identifier, `REQUIRED_TAGS`. For the `InputParameters` attribute, the tag keys that the rule requires, `CostCenter` and `Owner`, are specified.

If the command succeeds, AWS Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

**To add a customer managed Config rule**

The following command provides JSON code to add a customer managed Config rule:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` is a JSON file that contains the rule configuration:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
```

```
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

For the `ComplianceResourceTypes` attribute, this JSON code limits the scope to resources of the `AWS::EC2::Instance` type, so AWS Config will evaluate only EC2 instances against the rule. Because this rule is a customer managed rule, the `Owner` attribute is set to `CUSTOM_LAMBDA`, and the `SourceIdentifier` attribute is set to the ARN of the AWS Lambda function. The `SourceDetails` object is required. The parameters that are specified for the `InputParameters` attribute are passed to the AWS Lambda function when AWS Config invokes it to evaluate resources against the rule.

If the command succeeds, AWS Config returns no output. To verify the rule configuration, run the describe-config-rules command, and specify the rule name.

- For API details, see PutConfigRule in *AWS CLI Command Reference*.

Python

**SDK for Python (Boto3)**

> **Note**
>
> There's more on GitHub. Find the complete example and learn how to set up and run in the AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- For API details, see PutConfigRule in *AWS SDK for Python (Boto3) API Reference*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

## Use `PutDeliveryChannel` with a CLI

The following code examples show how to use `PutDeliveryChannel`.

CLI

## AWS CLI

### To create a delivery channel

The following command provides the settings for the delivery channel as JSON code:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

The `deliveryChannel.json` file specifies the delivery channel attributes:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

This example sets the following attributes:

`name` - The name of the delivery channel. By default, AWS Config assigns the name `default` to a new delivery channel.You cannot update the delivery channel name with the `put-delivery-channel` command. For the steps to change the name, see Renaming the Delivery Channel.`s3BucketName` - The name of the Amazon S3 bucket to which AWS Config delivers configuration snapshots and configuration history files.If you specify a bucket that belongs to another AWS account, that bucket must have policies that grant access permissions to AWS Config. For more information, see Permissions for the Amazon S3 Bucket.

`snsTopicARN` - The Amazon Resource Name (ARN) of the Amazon SNS topic to which AWS Config sends notifications about configuration changes.If you choose a topic from another account, the topic must have policies that grant access permissions to AWS Config. For more information, see Permissions for the Amazon SNS Topic.

`configSnapshotDeliveryProperties` - Contains the `deliveryFrequency` attribute, which sets how often AWS Config delivers configuration snapshots and how often it invokes evaluations for periodic Config rules.

If the command succeeds, AWS Config returns no output. To verify the settings of your delivery channel, run the describe-delivery-channels command.

- For API details, see PutDeliveryChannel in *AWS CLI Command Reference*.

PowerShell

**Tools for PowerShell V4**

**Example 1: This example changes the deliveryFrequency property of an existing delivery channel.**

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *AWS Tools for PowerShell Cmdlet Reference (V4)*.

**Tools for PowerShell V5**

**Example 1: This example changes the deliveryFrequency property of an existing delivery channel.**

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- For API details, see PutDeliveryChannel in *AWS Tools for PowerShell Cmdlet Reference (V5)*.

For a complete list of AWS SDK developer guides and code examples, see Using AWS Config with an AWS SDK. This topic also includes information about getting started and details about previous SDK versions.

# Document History

The following table describes the important changes to the documentation for AWS Config. For notification about updates to this documentation, you can subscribe to an RSS feed.

- **API version**: 2014-11-12
- **Latest documentation update**: January 09, 2026

| Change | Description | Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• cloudformation-stack-service-role-check<br>• cloudfront-distribution-key-group-enabled<br>• ecs-capacity-provider-termination-check<br>• ecs-task-definition-linux-user-non-root<br>• ecs-task-definition-windows-user-non-admin | January 9, 2026 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• aurora-global-database-encryption-at-rest<br>• cloudformation-termination-protection-check<br>• cognito-userpool-cust-auth-threat-full-check | December 8, 2025 |

| | | |
|---|---|---|
| | • cognito-user-pool-deletion-protection-enabled<br>• cognito-user-pool-mfa-enabled<br>• ebs-snapshot-block-public-access<br>• ecs-task-definition-efs-encryption-enabled<br>• ses-sending-tls-required | |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• aurora-global-database-encryption-at-rest<br>• cloudformation-termination-protection-check<br>• cognito-userpool-cust-auth-threat-full-check<br>• cognito-user-pool-deletion-protection-enabled<br>• cognito-user-pool-mfa-enabled<br>• ebs-snapshot-block-public-access<br>• ecs-task-definition-efs-encryption-enabled<br>• ses-sending-tls-required | December 8, 2025 |

| | | |
|---|---|---|
| ??? | The example Cross-Account S3 Bucket Policy no longer includes the `config.amazonaws.com` Service Principal. For more information, see required-permissions-cross-account. | December 3, 2025 |
| Security IAM updates | The `AWSConfigServiceRolePolicy` and `AWS_ConfigRole` policies now grants additional permissions for Amazon Lightsail and Amazon Simple Storage Service (Amazon S3). For more information, see AWS managed policies for AWS Config. | November 20, 2025 |
| Security IAM update | AWS Config has updated the managed policy `AWSConfigServiceRolePolicy` with enhanced documentation of comprehensive permissions for AWS resource configuration recording across over 100 AWS services. For information, see AWS Config updates to AWS managed policies. | November 11, 2025 |

| | | |
|---|---|---|
| Security IAM update | AWS Config has updated the managed policy `AWS_ConfigRole` with comprehensive permissions for AWS resource configuration recording across multiple services. For more information, see AWS managed policies for AWS Config. | November 10, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• amplify-app-no-environment-variables<br>• amplify-branch-description<br>• api-gwv2-stage-default-route-detailed-metrics-enabled<br>• apigateway-stage-description<br>• apigatewayv2-stage-description<br>• appconfig-deployment-strategy-tagged<br>• aps-rule-groups-namespace-tagged<br>• auditmanager-assessment-tagged<br>• batch-managed-spot-compute-environment-max-bid<br>• cognito-identity-pool-unauthenticated-logins<br>• customerprofiles-domain-tagged<br>• devicefarm-project-tagged<br>• devicefarm-test-grid-project-tagged<br>• ec2-network-insights-analysis-tagged<br>• eks-fargate-profile-tagged | October 27, 2025 |

- glue-ml-transform-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-video-stream-minimum-data-retention
- lambda-function-description
- lightsail-bucket-allow-public-overrides-disabled
- route53-resolver-firewall-domain-list-tagged
- route53-resolver-firewall-rule-group-association-tagged
- route53-resolver-firewall-rule-group-tagged
- route53-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-logs-enabled
- rum-app-monitor-tagged

| | | |
|---|---|---|
| AWS Config supports new resource types | With this release, you can use AWS Config to record configuration changes to new Amazon API Gateway, AWS CloudTrail, and AWS Config resource types. For more information, see Supported resource types. | October 10, 2025 |
| AWS Config supports new conformance pack | With this release, AWS Config supports the following conformance pack: Cyber Resilience Best Practices for Amazon S3, Amazon EBS, and Amazon DynamoDB | October 3, 2025 |

| | | |
|---|---|---|
| Security IAM updates | The `AWSConfigServiceRolePolicy` and `AWS_ConfigRole` policies now grants additional permissions for AWS Amplify, AWS AppSync, Amazon Bedrock, AWS CloudTrail, CloudFormation, AWS CodeArtifact, AWS CodePipeline, Amazon Connect, AWS Deadline Cloud, Amazon EC2, AWS Entity Resolution, AWS IoT SiteWise, Amazon IVS, AWS Lambda, Amazon EventBridge, Amazon Quick Suite, Amazon Redshift, Amazon Redshift Serverless, AWS Identity and Access Management Roles Anywhere, Amazon SageMaker, AWS Secrets Manager, Amazon Security Lake, AWS Service Catalog, AWS Shield, Amazon EC2 Systems Manager, and AWS WAFV2. For more information, see AWS managed policies for AWS Config. | October 1, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• cognito-user-pool-password-policy-check<br>• dms-replication-instance-multi-az-enabled<br>• ec2-launch-templates-ebs-volume-encrypted<br>• rds-mysql-cluster-copy-tags-to-snapshot-check<br>• rds-pgsql-cluster-copy-tags-to-snapshot-check | October 1, 2025 |
| AWS Config supports new resource types in the Asia Pacific (Taipei) Region region | With this release, AWS Config now supports the following AWS WAFV2 resource types in the Asia Pacific (Taipei) Region region:<br>• AWS::WAFv2::IPSet<br>• AWS::WAFv2::ManagedRuleSet<br>• AWS::WAFv2::RegexPatternSet<br>• AWS::WAFv2::RuleGroup<br>• AWS::WAFv2::WebACL<br><br>For more information, see Resource Coverage by Region Availability. | September 23, 2025 |

| | | |
|---|---|---|
| AWS Config updates conformance packs | With this release, AWS Config has updated the following conformance packs:<br>• Operational Best Practices for ACSC Essential 8<br>• Operational Best Practices for ACSC ISM - Part 2 | September 9, 2025 |
| AWS Config supports new resource types | With this release, you can use AWS Config to record configuration changes to new AWS CodeArtifact, AWS Config, AWS Glue, AWS Network Manager, and AWS Identity and Access Management resource types. For more information, see Supported resource types. | September 3, 2025 |
| AWS Config supports new resource types | With this release, you can use AWS Config to record configuration changes to new AWS Backup, Amazon OpenSearch Service, Amazon EC2, Amazon Managed Streaming for Apache Kafka, Amazon Redshift, Route 53 Profiles, AWS Systems Manager Incident Manager, AWS Transfer Family, and Amazon CloudFront resource types. For more information, see Supported resource types. | August 15, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• cloudfront-origin-lambda-url-oac-enabled<br>• sqs-queue-policy-full-access-check<br>• sqs-queue-dlq-check | August 14, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• alb-tagged<br>• api-gw-rest-api-tagged<br>• api-gw-stage-tagged<br>• appsync-graphql-api-xray-enabled<br>• cloudwatch-metric-stream-tagged<br>• codebuild-report-group-tagged<br>• datasync-location-object-storage-using-https<br>• ec2-vpn-connection-tagged<br>• ecs-capacity-provider-tagged<br>• efs-file-system-tagged<br>• eks-addon-tagged<br>• elb-internal-scheme-check<br>• elb-tagged<br>• glb-tagged<br>• iot-job-template-tagged<br>• iotdevicedefender-custom-metric-tagged<br>• kms-key-tagged<br>• msk-cluster-tagged<br>• nlb-tagged<br>• rds-event-subscription-tagged<br>• rds-option-group-tagged | August 13, 2025 |

- route53-health-check-tagged
- route53-hosted-zone-tagged
- service-catalog-portfolio-tagged
- stepfunctions-state-machine-tagged
- workspaces-connection-alias-tagged
- workspaces-workspace-tagged

| | | |
|---|---|---|
| Security IAM updates | The `AWS_ConfigRole` policy now grants additional permissions for AWS ARC - Zonal Shift, Amazon Bedrock, AWS CloudTrail, AWS CodeArtifact, AWS Deadline Cloud, AWS Database Migration Service, AWS Glue, AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka, AWS Lake Formation, Amazon CloudWatch Logs, AWS Elemental MediaLive, AWS Elemental MediaPackage, Amazon Relational Database Service, Amazon Simple Storage Service, AWS Secrets Manager, Amazon Security Lake, AWS Service Catalog, Amazon Simple Email Service, and AWS X-Ray. For more information, see AWS managed policies for AWS Config. | July 28, 2025 |

| | | |
|---|---|---|
| Security IAM updates | The `AWSConfigServiceRolePolicy` policy now grants additional permissions for AWS ARC - Zonal Shift, Amazon Bedrock, AWS CloudTrail, AWS CodeArtifact, AWS Deadline Cloud, AWS Database Migration Service, AWS Glue, AWS Identity and Access Management, Amazon Managed Streaming for Apache Kafka, AWS Lake Formation, Amazon CloudWatch Logs, AWS Elemental MediaLive, AWS Elemental MediaPackage, Amazon Relational Database Service, Amazon Simple Storage Service, AWS Secrets Manager, Amazon Security Lake, AWS Service Catalog, Amazon Simple Email Service, AWS X-Ray, and Amazon API Gateway. For more information, see AWS managed policies for AWS Config. | July 28, 2025 |

| | | |
|---|---|---|
| AWS Config supports new resource types | With this release, you can use AWS Config to record configuration changes to new AWS Backup, AWS Billing and Cost Management, CloudFormation, Amazon CloudFront, AWS Entity Resolution, AWS IoT, AWS Private Certificate Authority, Amazon Relational Database Service, and Amazon S3 resource types. For more information, see Supported resource types. | July 15, 2025 |
| Security IAM updates | The `AWS_ConfigRole` policy and `AWSConfigServiceRolePolicy` policy now grants additional permissions for AWS Backup gateway, AWS Billing and Cost Management, Amazon Bedrock, AWS CloudFormation, Amazon CloudFront, AWS Entity Resolution, AWS IoT Core Device Advisor, AWS Lambda, AWS Network Manager, AWS Private Certificate Authority, Amazon Redshift, Amazon S3 Tables, AWS Systems Manager Quick Setup. For more information, see AWS managed policies for AWS Config. | June 18, 2025 |

| | | |
|---|---|---|
| AWS Config supports new resource types | With this release, you can use AWS Config to record configuration changes to new Amazon Bedrock resource types. For more information, see Supported resource types. | June 17, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• cloudfront-ssl-policy-check<br>• cognito-identity-pool-unauth-access-check<br>• ec2-enis-source-destination-check-enabled<br>• elbv2-listener-encryption-in-transit<br>• lambda-function-xray-enabled<br>• msk-cluster-public-access-disabled<br>• msk-connect-connector-logging-enabled<br>• msk-unrestricted-access-check<br>• aurora-mysql-cluster-audit-logging<br>• redshift-cluster-multi-az-enabled<br>• s3express-dir-bucket-lifecycle-rules-check<br>• ssm-automation-logging-enabled<br>• ssm-automation-block-public-sharing | June 13, 2025 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Bedrock. For more information, see AWS managed policies for AWS Config. | May 27, 2025 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon App Integrations, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Inspector, Amazon Macie, Amazon Route 53 Profiles, Amazon OpenSearch Serverless, Amazon Simple Storage Service (Amazon S3), AWS Security Hub CSPM, and Amazon SageMaker AI resource types. For more information, see Supported Resource Types. | April 30, 2025 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: redshift-serverless-default-db-name-check | April 22, 2025 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: redshift-serverless-default-admin-check | April 17, 2025 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS B2B Data Interchange, Amazon Bedrock, AWS Clean Rooms, AWS CodeConnections, AWS Direct Connect, AWS Database Migration Service (AWS DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI, AWS Security Hub CSPM, and AWS Systems Manager Incident Manager, AWS Systems Manager Incident Manager Contacts, and AWS Systems Manager. For more information, see AWS managed policies for AWS Config. | April 8, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• s3-bucket-tagged<br>• ecr-repository-tagged<br>• sagemaker-feature-group-tagged<br>• sagemaker-domain-tagged<br>• cognito-user-pool-tagged | April 1, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• nlb-cross-zone-load-balancing-enabled<br>• redshift-serverless-publish-logs-to-cloudwatch<br>• rds-instance-subnet-igw-check<br>• ec2-spot-fleet-request-ct-encryption-at-rest<br>• redshift-serverless-workgroup-encrypted-in-transit<br>• redshift-serverless-workgroup-no-public-access<br>• redshift-serverless-namespace-cmk-encryption<br>• event-data-store-cmk-encryption-enabled<br>• ecs-task-definition-network-mode-not-host<br>• rds-proxy-tls-encryption<br>• nlb-logging-enabled<br>• redshift-audit-logging-enabled<br>• s3-lifecycle-policy-check<br>• sagemaker-image-tagged<br>• redshift-cluster-parameter-group-tagged<br>• ec2-dhcp-options-tagged<br>• sagemaker-app-image-config-tagged | March 22, 2025 |

- mariadb-publish-logs-to-cloudwatch-logs
- docdb-cluster-encrypted-in-transit
- rds-sqlserver-encrypted-in-transit
- ec2-traffic-mirror-session-tagged
- ec2-launch-template-tagged
- ec2-traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2-prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- sagemaker_notebook_instance_platform_version
- ec2-traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-logging
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encrypted-in-transit
- iam-saml-provider-tagged
- ec2-fleet-tagged
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2-network-insights-access-scope-tagged
- lightsail-certificate-tagged
- ec2-capacity-reservation-tagged
- ec2-transit-gateway-multicast-domain-tagged
- dms-endpoint-tagged
- ec2-carrier-gateway-tagged
- dms-replication-task-tagged
- ec2-client-vpn-endpoint-tagged
- lightsail-bucket-tagged
- ec2-network-insights-access-scope-analysis-tagged
- nlb-listener-tagged
- ec2-network-insights-path-tagged

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• docdb-cluster-encrypted-in-transit<br>• mariadb-publish-logs-to-cloudwatch-logs<br>• aurora-mysql-cluster-audit-logging<br>• rds-mariadb-instance-encrypted-in-transit<br>• rds-sqlserver-encrypted-in-transit<br>• sagemaker-notebook-instance-platform-version<br>• appstream-fleet-multi-az<br>• apprunner-vpc-connector-multi-az<br>• mq-broker-general-logging-enabled<br>• mq-active-single-instance-broker-storage-type-efs<br>• mq-active-broker-ldap-authentication<br>• iottwinmaker-component-type-tagged | March 19, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• fsx-openzfs-deployment-type-check<br>• fsx-ontap-deployment-type-check<br>• fsx-windows-deployment-type-check<br>• redshift-serverless-workgroup-routes-within-vpc | March 18, 2025 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules: ec2-instance-launched-with-allowed-ami | March 11, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• connect-instance-logging-enabled<br>• ecr-repository-cmk-encryption-enabled<br>• elbv2-predefined-security-policy-ssl-check<br>• glue-spark-job-supported-version<br>• guardduty-runtime-monitoring-enabled<br>• guardduty-ecs-protection-runtime-enabled<br>• guardduty-ec2-protection-runtime-enabled<br>• netfw-subnet-change-protection-enabled<br>• rds-sql-server-logs-to-cloudwatch<br>• sqs-queue-no-public-access<br>• transfer-connector-logging-enabled | March 7, 2025 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Elastic Compute Cloud (Amazon EC2). For more information, see AWS managed policies for AWS Config. | March 4, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• athena-workgroup-description<br>• amplify-app-tagged<br>• sagemaker-app-image-config-tagged<br>• elasticbeanstalk-application-version-description<br>• amplify-branch-performance-mode-enabled<br>• athena-workgroup-engine-version-auto-upgrade<br>• sagemaker-image-description<br>• devicefarm-instance-profile-tagged<br>• transfer-workflow-description<br>• ec2-traffic-mirror-session-tagged<br>• appstream-fleet-in-vpc<br>• transfer-agreement-tagged<br>• ec2-traffic-mirror-target-description<br>• transfer-agreement-description<br>• athena-prepared-statement-description | February 8, 2025 |

- batch-managed-compute-env-compute-resources-tagged
- codedeploy-deployment-group-auto-rollback-enabled
- batch-managed-compute-environment-using-launch-template
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-configuration
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk-tagged
- transfer-profile-tagged
- ec2-traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-not-empty
- elasticbeanstalk-application-description

- codedeploy-deployment-group-outdated-instances-update
- ec2-launch-template-tagged
- fis-experiment-template-tagged
- ivs-channel-playback-authorization-enabled
- redshift-cluster-parameter-group-tagged
- ec2-traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-configuration-exists
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-deletion-enabled
- appconfig-hosted-configuration-version-description
- appconfig-freeform-profile-config-storage
- datasync-task-data-verification-enabled

| | | |
|---|---|---|
| | • apprunner-service-observability-enabled<br>• transfer-certificate-description<br>• appconfig-deployment-strategy-replicate-to-ssm<br>• transfer-workflow-tagged<br>• transfer-connector-tagged<br>• ec2-traffic-mirror-session-description<br>• customerprofiles-object-type-allow-profile-creation<br>• sagemaker-image-tagged | |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Simple Storage Service (Amazon S3) resource types. For more information, see Supported Resource Types. | February 6, 2025 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Simple Storage Service (Amazon S3) resource types. For more information, see Supported Resource Types. | January 29, 2025 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2), AWS HealthOmics, Amazon Simple Storage Service (Amazon S3), and Amazon Simple Email Service (Amazon SES). For more information, see AWS managed policies for AWS Config. | January 16, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• appmesh-mesh-deny-tcp-forwarding<br>• sagemaker-model-isolation-enabled<br>• evidently-project-description<br>• alb-internal-scheme-check<br>• evidently-segment-description<br>• appconfig-environment-description<br>• apprunner-service-in-vpc<br>• sagemaker-domain-in-vpc<br>• nlb-internal-scheme-check<br>• emr-security-configuration-encryption-rest<br>• apprunner-service-no-public-access<br>• sagemaker-model-in-vpc<br>• appconfig-deployment-strategy-description<br>• evidently-launch-description<br>• iot-authorizer-token-signing-enabled | January 9, 2025 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2) resource types. For more informati on, see Supported Resource Types. | January 9, 2025 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• batch-job-queue-tagged<br>• iottwinmaker-sync-job-tagged<br>• codeguruprofiler-profiling-group-tagged<br>• ivs-recording-configuration-tagged<br>• iottwinmaker-entity-tagged<br>• iottwinmaker-workspace-tagged<br>• iottwinmaker-scene-tagged<br>• acmpca-certificate-authority-tagged<br>• appflow-flow-tagged<br>• iotevents-detector-model-tagged<br>• appmesh-virtual-node-logging-file-path-exists<br>• apprunner-vpc-connector-tagged<br>• apprunner-service-tagged<br>• iotwireless-fuota-task-tagged<br>• appmesh-virtual-node-backend-defaults-tls-on<br>• codegururreviewer-repository-association-tagged<br>• iotevents-input-tagged | January 8, 2025 |

- appmesh-virtual-gateway-logging-file-path-exists
- batch-compute-environment-tagged
- batch-scheduling-policy-tagged
- customerprofiles-object-type-tagged
- emr-security-configuration-encryption-transit
- iotwireless-service-profile-tagged
- ivs-playback-key-pair-tagged
- cassandra-keyspace-tagged
- iotevents-alarm-model-tagged
- appconfig-application-description
- appmesh-virtual-gateway-backend-defaults-tls
- ivs-channel-tagged
- iotwireless-multicast-group-tagged

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2), Amazon Cognito, AWS Elemental MediaConnect, and Amazon OpenSearch Service resource types. For more informati on, see Supported Resource Types. | December 19, 2024 |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy now grants additional permissions for AWS Organizations. For more information, see AWS managed policies for AWS Config. | December 18, 2024 |
| AWS Config supports service-linked configuration recorders | With this release, AWS Config supports service-linked configuration recorders. You enable a service-linked configuration recorder in the supported service or using the AWS CLI, and the recorder records the resource types needed for the linked service on your behalf. You can view details of a service-linked configuration recorder using the AWS Config console or AWS CLI. For more informati on, see Working with the configuration recorder. | November 27, 2024 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• appconfig-application-tagged<br>• appconfig-configuration-profile-tagged<br>• appconfig-environment-tagged<br>• appconfig-extension-association-tagged<br>• appmesh-gateway-route-tagged<br>• appmesh-mesh-tagged<br>• appmesh-route-tagged<br>• appmesh-virtual-gateway-tagged<br>• appmesh-virtual-node-tagged<br>• appmesh-virtual-router-tagged<br>• appmesh-virtual-service-tagged<br>• evidently-launch-tagged<br>• evidently-project-tagged<br>• evidently-segment-tagged<br>• frauddetector-entity-type-tagged<br>• frauddetector-label-tagged<br>• frauddetector-outcome-tagged | November 12, 2024 |

- frauddetector-variable-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS AppConfig, AWS CloudTrail, Amazon Connect, Amazon DataZone, Amazon DevOps Guru, AWS Glue, Identity Store, AWS IoT, AWS IoT FleetWise, AWS IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, AWS Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler, AWS Systems Manager, and Amazon VPC Lattice. For more information, see AWS managed policies for AWS Config. | November 8, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: cognito-user-pool-advanced-security-enabled | November 6, 2024 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• active-mq-supported-version<br>• rabbit-mq-supported-version<br>• ec2-vpn-connection-logging-enabled<br>• appsync-cache-ct-encryption-at-rest<br>• appsync-cache-ct-encryption-in-transit<br>• vpc-endpoint-enabled<br>• efs-filesystem-ct-encrypted<br>• redshift-cluster-subnet-group-multi-az<br>• sns-topic-no-public-access<br>• rabbit-mq-supported-version<br>• kms-key-policy-no-public-access<br>• rds-mysql-instance-encrypted-in-transit<br>• rds-postgres-instance-encrypted-in-transit<br>• rds-sql-server-logs-to-cloudwatch<br>• ec2-launch-template-imdsv2-check | October 21, 2024 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for PCI DSS 4.0 (Excluding global resource types)<br>• Operational Best Practices for PCI DSS 4.0 (Including global resource types) | September 23, 2024 |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon OpenSearch Service Severless, Amazon AppStream, AWS Backup, AWS CloudTrail, AWS Glue, EC2 Image Builder, AWS IoT, Amazon Interactive Video Service (Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTail or, AWS HealthOmics, and Amazon EventBridge Scheduler. For more information, see AWS managed policies for AWS Config. | September 16, 2024 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• ec2-resources-in-logically-air-gapped-vault<br>• ebs-resources-in-logically-air-gapped-vault<br>• aurora-resources-in-logically-air-gapped-vault<br>• efs-resources-in-logically-air-gapped-vault<br>• s3-resources-in-logically-air-gapped-vault<br>• storagegateway-resources-in-logically-air-gapped-vault<br>• virtualmachine-resources-in-logically-air-gapped-vault | September 3, 2024 |
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for FedRAMP (High Part 1)<br>• Operational Best Practices for FedRAMP (High Part 2) | August 27, 2024 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• athena-workgroup-logging-enabled<br>• codebuild-report-group-encrypted-at-rest<br>• cognito-user-pool-advanced-security-enabled<br>• datasync-task-logging-enabled<br>• efs-automatic-backups-enabled<br>• glue-job-logging-enabled<br>• glue-ml-transform-encrypted-at-rest<br>• kinesis-stream-backup-retention-check<br>• rds-aurora-postgresql-logs-to-cloudwatch<br>• rds-postgresql-logs-to-cloudwatch<br>• workspaces-root-volume-encryption-enabled<br>• workspaces-user-volume-encryption-enabled | July 22, 2024 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Elastic File System (Amazon EFS), Amazon Redshift and AWS Systems Manager for SAP. For more information, see AWS managed policies for AWS Config. | June 17, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• cloudtrail-s3-bucket-public-access-prohibited<br>• cloudtrail-s3-bucket-access-logging | May 8, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: iam-external-access-analyzer-enabled | May 2, 2024 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• guardduty-malware-protection-enabled<br>• guardduty-rds-protection-enabled<br>• guardduty-s3-protection-enabled<br>• inspector-lambda-standard-scan-enabled | April 26, 2024 |
| AWS Config simplifies usage analysis with Amazon CloudWatch | With this release, the Amazon CloudWatch metrics for monitoring AWS Config data usage will display only billable usage. This means, non-billable usage will no longer be displayed in both the Amazon CloudWatch metrics emitted to AWS Config and the AWS Config console. This allows you to validate AWS Config setup and usage using Amazon CloudWatch metrics and correlate billable usage with associated costs. For more information, see AWS Config Usage and Success Metrics. | April 26, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: iam-server-certificate-expiration-check | April 23, 2024 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• vpc-sg-port-restriction-check<br>• cloudtrail-all-write-s3-data-event-check<br>• cloudtrail-all-read-s3-data-event-check | April 17, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• guardduty-eks-protection-audit-enabled<br>• guardduty-eks-protection-runtime-enabled<br>• guardduty-lambda-protection-enabled<br>• inspector-ec2-scan-enabled<br>• inspector-ecr-scan-enabled<br>• inspector-lambda-code-scan-enabled<br>• redshift-unrestricted-port-access | April 16, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: efs-mount-target-public-accessible | March 20, 2024 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• dms-neptune-iam-authorization-enabled<br>• dms-mongo-db-authentication-enabled<br>• dms-redis-tls-enabled<br>• dax-tls-endpoint-encryption<br>• eks-cluster-secrets-encrypted<br>• kinesis-firehose-delivery-stream-encrypted<br>• mq-cloudwatch-audit-log-enabled<br>• mq-cloudwatch-audit-log-enabled<br>• opensearch-primary-node-fault-tolerance<br>• sagemaker-endpoint-config-prod-instance-count<br>• service-catalog-shared-within-organization<br>• transfer-family-server-no-ftp | February 26, 2024 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, AWS Glue, AWS Identity and Access Management (IAM), AWS Lambda, AWS RAM, Amazon Redshift Serverless, Amazon SageMaker AI, and Amazon Simple Notification Service (Amazon SNS). For more information, see AWS managed policies for AWS Config. | February 22, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: s3-bucket-cross-region-replication-enabled | February 12, 2024 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new AWS AppConfig, Amazon CloudWatch Evidently, AWS Identity and Access Management (IAM), Amazon MemoryDB (MemoryDB), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Redshift, and AWS Transfer Family resource types. For more informati on, see Supported Resource Types. | February 6, 2024 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rule: macie-auto-sensitive-data-discovery-check | January 29, 2024 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon AppStream, AWS Key Management Service (AWS KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon EC2), EC2 Image Builder, AWS Ground Station, AWS Mainframe Modernization, Amazon Quick Suite, Amazon Redshift, and AWS Systems Manager resource types. For more information, see Supported Resource Types. | January 3, 2024 |
| Service limits increase for the maximum number of AWS Config Rules per Region per account | With this release, AWS Config supports 1000 AWS Config rules per AWS Region per account. This increase applies to the total of all deployed rules including AWS Config managed rules, AWS Config custom rules, AWS Config conformance packs, AWS Security Hub CSPM controls, AWS Firewall Manager policies, and AWS Backup backup plans per Region per account. For more informati on, see Service Limits. | December 19, 2023 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• s3-meets-restore-time-target<br>• ebs-meets-restore-time-target<br>• ec2-meets-restore-time-target<br>• rds-meets-restore-time-target<br>• efs-meets-restore-time-target<br>• fsx-meets-restore-time-target<br>• aurora-meets-restore-time-target<br>• dynamodb-meets-restore-time-target | December 19, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS AppConfig, Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs, AWS Organizations, and Amazon Simple Storage Service (Amazon S3). For more information, see AWS managed policies for AWS Config. | December 5, 2023 |

| | | |
|---|---|---|
| Preview release: Natural language query processor for advanced queries | With this release, you can use the natural language query processor for advanced queries, which uses generative artificial intelligence (generati ve AI) capabilities that allow you to ask questions in plain English and convert them into a ready-to-use query format. With the natural language query processor, you can query your AWS account or across an AWS organizat ion. For more information, see Natural language query processor for advanced queries. | November 26, 2023 |

| | | |
|---|---|---|
| Periodic recording | With this release, AWS Config supports periodic recording. Periodic recording provides you with the ability to capture the latest configuration changes for your resources over a fixed period of time. You can now set the default frequency for the configuration recorder to Daily, allowing you to receive a configuration item (CI) representing the most recent state of your resources over the last 24-hour period, only if it's different from the previous CI recorded. The AWS Config console also introduces a new recording strategy experience, where you can also override the recording frequency for specific resource types or exclude specific resource types from recording. This can help make your settings fit your granular requirements.<br><br>The following data types are added:<br><br>• RecordingMode<br>• RecordingModeOverride<br><br>The following data types are updated: | November 26, 2023 |

- PutConfigurationRecorder
- ConfigurationRecorder
- BaseConfigurationItem
- ConfigurationItem

The following pages in the developer guide are updated:

- Recoding AWS Resources
- Setting up AWS Config with the AWS Config Console | 1-click setup
- Setting up AWS Config with the AWS Config Console | Manual setup
- Setting up AWS Config with the AWS CLI

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station, AWS Mainframe Modernization, Amazon MemoryDB, AWS Organizations, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53, AWS Service Catalog, and AWS Transfer Family.<br><br>The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy also now add security identifiers (SID) for `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` , and `AWSConfigServiceRolePolicy` policy. | November 17, 2023 |

| | | |
|---|---|---|
| | For more information, see AWS managed policies for AWS Config. | |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• acm-pca-root-ca-disabled<br>• dynamodb-table-deletion-protection-enabled<br>• ec2-client-vpn-connection-log-enabled<br>• eks-cluster-log-enabled<br>• emr-block-public-access<br>• fsx-windows-audit-log-configured<br>• fsx-openzfs-copy-tags-enabled<br>• fsx-lustre-copy-tags-to-backups<br>• msk-enhanced-monitoring-enabled<br>• mq-auto-minor-version-upgrade-enabled<br>• neptune-cluster-multi-az-enabled<br>• opensearch-update-check<br>• s3-access-point-in-vpc-only<br>• s3-access-point-public-access-blocks<br>• s3-bucket-mfa-delete-enabled | November 9, 2023 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new AWS Identity and Access Management (IAM), AWS Network Manager, AWS Private Certificate Authority (AWS Private CA), AWS App Mesh, Amazon Connect, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), AWS IoT, AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka Connect (Amazon MSK Connect), AWS Lambda, and AWS Resource Explorer resource types. For more information, see Supported Resource Types. | November 3, 2023 |
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance pack: Operational Best Practices for BNM RMiT | October 26, 2023 |

| | | |
|---|---|---|
| Compliance and Inventory Dashboards for Aggregators | With this release, AWS Config adds a compliance dashboard page and an inventory dashboard page to the aggregated view in the AWS Config console.<br><br>For the compliance dashboard page, you can view automated dashboards with widgets that summarize insights on resource compliance within your aggregator, such as Top 10 resource types by noncompliant resources, Top 10 account level conformance packs by noncompliant rules, and more.<br><br>For the inventory dashboard page, you can view automated dashboard with widgets that summarize insights on resource configuration data within your aggregator, such as Top 10 resource types by resource count, Top 10 accounts by resource count, and more.<br><br>For information on the graph and charts, see Compliance dashboard and Inventory dashboard. | October 23, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS Private CA, AWS App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty, Amazon Inspector, AWS IoT, AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK), AWS Lambda, AWS Network Manager, AWS Organizations, and Amazon SageMaker AI. For more information, see AWS managed policies for AWS Config. | October 4, 2023 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new AWS IoT, AWS IoT TwinMaker, AWS IoT Wireless, Amazon Personalize Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon SageMaker AI, AWS CodeBuild, Amazon AppStream, and Amazon Inspector resource types. For more information, see Supported Resource Types. | October 4, 2023 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• docdb-cluster-deletion-protection-enabled<br>• docdb-cluster-audit-logging-enabled<br>• docdb-cluster-snapshot-public-prohibited<br>• mq-active-deployment-mode<br>• mq-rabbit-deployment-mode<br>• dms-auto-minor-version-upgrade-check<br>• dms-replication-task-target db-logging<br>• dms-replication-task-source db-logging<br>• dms-endpoint-ssl-configured<br>• custom-eventbus-policy-attached<br>• global-endpoint-event-replication-enabled<br>• route53-query-logging-enabled<br>• rds-aurora-mysql-audit-logging-enabled<br>• rds-cluster-auto-minor-version-upgrade-enable<br>• appsync-authorization-check | September 21, 2023 |

| | | |
|---|---|---|
| | • netfw-deletion-protection-enabled<br>• wafv2-rulegroup-logging-enabled<br>• msk-in-cluster-node-require-tls | |
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance packs:<br>• Operational Best Practices for Amazon S3<br>• Operational Best Practices for EC2 | September 8, 2023 |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy now removes permissions for AWS Systems Manager (Systems Manager). For more information, see AWS managed policies for AWS Config. | September 6, 2023 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon CodeGuru Profiler, AWS Elemental MediaConnect, AWS Transfer Family, Amazon Managed Service for Prometheus, AWS Batch, AWS Cloud Map, and Amazon Route 53 Resolver resource types. For more information, see Supported Resource Types. | September 6, 2023 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• athena-workgroup-encrypted-at-rest<br>• neptune-cluster-iam-database-authentication<br>• neptune-cluster-copy-tags-to-snapshot-enabled<br>• neptune-cluster-cloudwatch-log-export-enabled<br>• neptune-cluster-deletion-protection-enabled<br>• neptune-cluster-snapshot-encrypted<br>• neptune-cluster-backup-retention-check<br>• neptune-cluster-encrypted<br>• neptune-cluster-snapshot-public-prohibited<br>• docdb-cluster-backup-retention-check<br>• docdb-cluster-encrypted<br>• rds-cluster-encrypted-at-rest | August 10, 2023 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new AWS Amplify, Amazon AppIntegrations, AWS App Mesh, Amazon Athena, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS IoT Greengrass Version 2, AWS Ground Station, AWS Elemental MediaConvert, AWS Elemental MediaTailor, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Personalize, Amazon Pinpoint, and AWS Resilience Hub resource types. For more information, see Supported Resource Types. | August 3, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for AWS App Mesh, Amazon WorkSpaces Applications, AWS CloudFormation, Amazon CloudFront AWS CodeArtifact, AWS CodeBuild, Amazon Connect, AWS Glue, Amazon GuardDuty, AWS Identity and Access Management (IAM), Amazon Inspector, AWS IoT, AWS IoT TwinMaker, AWS IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, AWS Network Manager, AWS Organizations, AWS Resource Explorer, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), and Amazon EC2 Systems Manager (SSM). For more information, see AWS managed policies for AWS Config. | July 28, 2023 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Kinesis, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon Connect, AWS CloudFormation, AWS AppConfig, AWS App Mesh, AWS App Runner, and AWS Database Migration Service (AWS DMS) resource types. For more information, see Supported Resource Types. | July 10, 2023 |
| Service limits increase for organization conformance packs | With this release, AWS Config supports 350 AWS Config rules per region per account across all conformance packs and 350 organizational AWS Config rules per organization. For more information, see Service Limits. | June 13, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for AWS Amplify, Amazon Connect, AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, AWS Batch, AWS CloudFormation, AWS CloudTrail, AWS CodeArtifact, Amazon CodeGuru, AWS Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Organizations, AWS IoT Greengrass, AWS Ground Station, AWS Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon Quick Suite, AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon | June 13, 2023 |

S3), Amazon SageMaker AI, and AWS Transfer Family. For more information, see AWS managed policies for AWS Config.

| | | |
|---|---|---|
| AWS Config Recording Exclusions by Resource Type | With this release, AWS Config allows you to exclude specific types of AWS resources from inventory tracking and compliance monitoring while still tracking all other supported resource types currently available in AWS Config, including those that will be added in the future. You can use this feature to concentrate on critical resources that are subject to your compliance and governance standards.<br><br>The updates to the API for the configuration recorder and recording group are backward compatible, meaning that they work with previous versions of the PutConfigurationRecorder API. You can continue to manage which resource types are recorded in the exact same way as before without using the updated or new APIs.<br><br>The following data types are added:<br><br>• RecordingStrategy<br>• ExclusionByResourceTypes<br><br>The following data types are updated: | June 9, 2023 |

| | | |
|---|---|---|
| | • PutConfigurationRecorder<br>• ConfigurationRecorder<br>• RecordingGroup<br><br>The following page in the developer guide is updated:<br><br>• Selecting Which Resources are Recorded | |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Container Service (Amazon ECS), Amazon Keyspaces (for Apache Cassandra) (Amazon Keyspaces), AWS Signer, AWS Amplify, AWS App Mesh, AWS App Runner, Amazon WorkSpaces Applications, AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Identity and Access Management (IAM), Amazon Pinpoint, Amazon SageMaker AI, AWS Transfer Family, Amazon Data Firehose resource types. For more information, see Supported Resource Types. | June 5, 2023 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• cloudfront-s3-origin-access-control-enabled<br>• custom-schema-registry-policy-attached<br>• ec2-client-vpn-not-authorize-all<br>• elasticache-supported-engine-version<br>• macie-status-check<br>• mq-automatic-minor-version-upgrade-enabled<br>• mq-cloudwatch-audit-logging-enabled<br>• netfw-logging-enabled<br>• opensearch-encrypted-at-res<br>• step-functions-state-machine-logging-enabled | May 10, 2023 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Route 53 Resolver, Amazon Elastic Compute Cloud (Amazon EC2), AWS IoT Wireless, AWS Network Manager, AWS Device Farm, AWS Ground Station, Amazon AppFlow, Amazon Redshift, Amazon Pinpoint, AWS IoT, AWS AppConfig, EC2 Image Builder, Amazon CloudWatch, AWS Panorama, Amazon SageMaker Runtime, Amazon ECR, and AWS Audit Manager resource types. For more information, see Supported Resource Types. | May 5, 2023 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to `AWS::NetworkFirewall::TLSInspectionConfiguration`. For more information, see Supported Resource Types. | May 1, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for AWS Amplify, AWS App Mesh, AWS App Runner, Amazon CloudFront, AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, AWS Transfer Family, Amazon Pinpoint, AWS Migration Hub, AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service, and AWS WAF. For more information, see AWS managed policies for AWS Config. | April 13, 2023 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• elasticache-auto-minor-version-upgrade-check<br>• elasticache-repl-grp-auto-failover-enabled<br>• elasticache-repl-grp-encrypted-at-rest<br>• elasticache-repl-grp-encrypted-in-transit<br>• elasticache-repl-grp-redis-auth-enabled<br>• elasticache-subnet-group-check<br>• cloudfront-s3-origin-non-existent-bucket | April 10, 2023 |
| Service limits increase for organization conformance packs | With this release, AWS Config supports 350 AWS Config rules per account across all organization conformance packs. For more information, see Service Limits. | April 3, 2023 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• acm-certificate-rsa-check<br>• appsync-associated-with-waf<br>• appsync-logging-enabled<br>• elasticache-rbac-auth-enabled<br>• mq-no-public-access<br>• netfw-multi-az-enabled<br>• ses-malware-scanning-enabled<br>• eks-cluster-logging-enabled<br>• appsync-cache-encryption-at-rest | April 3, 2023 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon WorkSpace s Applications, AWS Auto Scaling, Amazon Connect Amazon Elastic Compute Cloud, Amazon EventBrid ge, HealthLake, Kinesis video stream, AWS IoT TwinMaker, Lookout for Vision, Network Manager, Amazon Pinpoint, Amazon Application Recovery Controller (ARC), and AWS RoboMaker resource types. For more information, see Supported Resource Types. | April 3, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for Amazon AppFlow, AWS App Runner, Amazon WorkSpaces Applications, AWS CloudFormation, Amazon CloudFront, Amazon CloudWatch, AWS CodeArtifact, AWS CodeCommit, AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Ground Station, AWS Identity and Access Management (IAM), AWS IoT, Amazon MemoryDB, Amazon Pinpoint, AWS Network Manager, AWS Panorama, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon SageMaker AI. For more information, see AWS managed policies for AWS Config. | March 30, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS Audit Manager. For more information, see AWS managed policies for AWS Config. | March 3, 2023 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new AWS Elemental MediaPackage, Amazon EventBridge, AWS IoT, (Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Lookout for Metrics, Amazon Lex, AWS Budgets, AWS Device Farm, Amazon CodeGuru Reviewer, Amazon Route 53 Resolver, and AWS RoboMaker resource types. For more information, see Supported Resource Types. | March 2, 2023 |
| Security IAM update | AWS Config now tracks changes to the `AWSConfigMultiAccountSetupPolicy` policy. For more information, see AWS managed policies for AWS Config. | February 27, 2023 |

| | | |
|---|---|---|
| AWS Config Resource Coverage by Region Availability | With this release, AWS Config provides Region information for each supported resource type. For information on which resource types are supported in which Regions, see Resource Coverage by Region Availability. | February 20, 2023 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Interactive Video Service (Amazon IVS), Amazon Simple Storage Service (Amazon S3), AWS Glue, Amazon Elastic Kubernetes Service (Amazon EKS), AWS IoT, Amazon Relational Database Service (Amazon RDS), and Managed Service for Apache Flink resource types. For more information, see Supported Resource Types. | February 7, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon WorkSpaces Applications, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC), AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty, and Amazon CloudWatch Logs. For more information, see AWS managed policies for AWS Config. | February 1, 2023 |
| Security IAM update | As a security best practice, the `ConfigConformsServiceRolePolicy` policy now removes broad resource-level permission for `config:DescribeConfigRules` . For more information, see AWS managed policies for AWS Config. | January 12, 2023 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail , AWS Elemental MediaPackage, AWS Network Manager, Amazon Quick Suite, AWS Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3), and Amazon Timestream. For more information, see AWS managed policies for AWS Config. | January 10, 2023 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon MQ, AWS AppConfig, AWS Cloud9, Amazon EventBridge schemas, Amazon Fraud Detector, AWS IoT, AWS IoT Analytics, Amazon Lightsail, AWS Elemental MediaPackage (MediaPackage), Amazon Application Recovery Controller (ARC), AWS Resilience Hub, and AWS Transfer Family resource types. For more information, see Supported Resource Types. | January 5, 2023 |
| AWS Config rule resource coverage | With this release, AWS Config displays the resource type coverage for an increased number of AWS Config managed rules. | December 21, 2022 |
| AWS Config rule discoverability | With this release, AWS Config supports pages for List of AWS Config Managed Rules by Evaluation Mode, List of AWS Config Managed Rules by Trigger Type, and List of AWS Config Managed Rules by Region Availability. | December 21, 2022 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance packs:<br>• Operational Best Practices for K-ISMS<br>• Operational Best Practices for NIST 800 171<br>• Operational Best Practices for PCI DSS 3.2.1<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) High<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low<br>• Operational Best Practices for NZISM<br>• Operational Best Practices for NIST 800-53 rev 5 | December 19, 2022 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• api-gwv2-access-logs-enabled<br>• api-gwv2-authorization-type-configured<br>• cloudfront-security-policy-check<br>• ec2-launch-template-public-ip-disabled<br>• elastic-beanstalk-logs-to-cloudwatch<br>• sagemaker-notebook-instance-inside-vpc<br>• sagemaker-notebook-instance-root-access-check<br>• security-account-information-provided<br>• storagegateway-resources-protected-by-backup-plan<br>• wafv2-rulegroup-not-empty<br>• wafv2-webacl-not-empty | December 9, 2022 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon CloudWatch RUM, Amazon EventBridge, Amazon GuardDuty, Amazon Simple Email Service (Amazon SES), AWS Backup, AWS DataSync, and AWS Fault Injection Service (AWS FIS) resource types. For more informati on, see Supported Resource Types. | December 9, 2022 |

| | | |
|---|---|---|
| AWS Config Proactive Compliance | With this release, AWS Config supports the ability to proactively check for compliance with AWS Config rules before resource provisioning. This allows you to evaluate the configuration settings of your resources before they are created or updated. Use AWS Config to track the configuration changes made to your resources, either pre-provisioning or post-provisioning, and check if your resources match your desired configurations.<br><br>The following data types are added:<br><br>• GetResourceEvaluationSummary<br>• StartResourceEvaluation<br>• ListResourceEvaluations<br><br>The following data types are updated:<br><br>• DescribeConfigRulesFilters<br>• GetComplianceDetailsByResource<br>• EvaluationResultQualifier<br>• EvaluationModeConfiguration | November 28, 2022 |

The following pages in the developer guide are updated:

- Components of an AWS Config Rule
- Evaluation Mode and Trigger Types for AWS Config Rules
- AWS Config Managed Rules
- AWS Config Custom Rules
- Managing Your AWS Config Rules

| | | |
|---|---|---|
| Drift Detection as Configuration Item (CI) for the AWS Config Configuration Recorder | With this release, AWS Config tracks all changes to the configuration recorder to indicate if the state of the configuration recorder differs, or has *drifted*, from its previous state; for example, if there are updates to resource types that you have enabled AWS Config to track, if you have stopped or started the configuration recorder, or if you have deleted or uninstalled the configuration recorder. The `AWS::Config::ConfigurationRecorder` resource type is a system resource type of AWS Config and recording of this resource type is enabled by default in all supported Regions. Recording for the `AWS::Config::ConfigurationRecorder` resource type comes with no additional charge. For more information, see Drift Detection for the Configuration Recorder. | November 18, 2022 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new AWS IoT Events, AWS Cloud Map, EC2 Image Builder, AWS DataSync, AWS Glue, Amazon Application Recovery Controller (ARC), and Amazon Elastic Container Registry (Amazon ECR) resource types. For more information, see Supported Resource Types. | November 8, 2022 |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS CloudFormation. For more information, see AWS managed policies for AWS Config. | November 7, 2022 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for Criminal Justice Information Services (CJIS)<br>• Security Best Practices for Amazon SageMaker AI<br>• Security Best Practices for Amazon Elastic Container Registry<br><br>The following conformance packs are updated:<br>• Operational Best Practices for MAS TRMG<br>• Operational Best Practices for NCSC Cyber Assesment Framework<br>• Operational Best Practices for NCSC Cloud Security Principles | October 27, 2022 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS Certificate Manager, Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect, AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift Servers, Amazon Location Service, AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon Quick Suite, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), AWS Cloud Map, and AWS Security Token Service. For more informati | October 19, 2022 |

| | | |
|---|---|---|
| | on, see AWS managed policies for AWS Config. | |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Email Service (Amazon SES), AWS AppConfig, AWS Cloud Map, and AWS DataSync resource types. For more information, see Supported Resource Types. | October 6, 2022 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon GuardDuty, Amazon SageMaker AI, AWS AppSync, AWS Cloud Map, and AWS DataSync resource types. For more information, see Supported Resource Types. | October 4, 2022 |
| AWS Config supports new conformance pack | With this release, AWS Config updates the Operational Best Practices for SWIFT CSP conformance pack. | October 4, 2022 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for CMMC 2.0 Level 1<br>• Operational Best Practices for CMMC 2.0 Level 2<br><br>The following conformance packs are updated:<br>• Operational Best Practices for Amazon API Gateway<br>• Operational Best Practices for AWS Well-Architected Framework Reliability Pillar<br>• Operational Best Practices for AWS Well-Architected Framework Security Pillar<br>• Operational Best Practices for CMMC Level 1<br>• Operational Best Practices for CMMC Level 2<br>• Operational Best Practices for CMMC Level 3<br>• Operational Best Practices for CMMC Level 4<br>• Operational Best Practices for CMMC Level 5<br>• Operational Best Practices for FFIEC<br>• Operational Best Practices for FedRAMP(Low) | September 30, 2022 |

| | | |
|---|---|---|
| | • Operational Best Practices for MAS Notice 655<br>• Operational Best Practices for NBC TRMG<br>• Operational Best Practices for NIST 800 172 | |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS Glue. For more information, see AWS managed policies for AWS Config. | September 14, 2022 |
| AWS Config supports new conformance pack | With this release, AWS Config supports the Operational Best Practices for SWIFT CSP conformance pack. | September 9, 2022 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge Schemas, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon Quick Suite, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver, | September 7, 2022 |

Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer, AWS Cloud9, AWS Directory Service, AWS DataSync, AWS Elemental MediaPackage, AWS Glue, AWS IoT, AWS IoT Analytics , AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker , AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, and AWS Transfer Family. For more information, see AWS managed policies for AWS Config.

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for Amazon CloudWatch<br>• Operational Best Practices for Germany Cloud Computing Compliance Controls Catalog (C5)<br>• Operational Best Practices for IRS 1075<br><br>The following conformance packs are updated:<br>• AWS Control Tower Detective Guardrails Conformance Pack<br>• Operational Best Practices for CISA Cyber Essentials<br>• Operational Best Practices for ENISA Cybersecurity guide for SMEs<br>• Operational Best Practices for FDA Title 21 CFR Part 11<br>• Operational Best Practices for FedRAMP(Moderate)<br>• Operational Best Practices for HIPAA Security<br>• Operational Best Practices for NIST Privacy Framework v1.0<br>• Operational Best Practices for NYDFS 23 | August 31, 2022 |

| | | |
|---|---|---|
| | • Operational Best Practices for RBI Cyber Security Framework for UCBs<br>• Operational Best Practices for RBI MD-ITF | |
| Getting Started with AWS Config and Custom Conformance Pack updates | With this release, AWS Config updates the Getting Started with AWS Config and Setting Up AWS Config with the Console pages, introducing a 1-click setup and Manual setup page. AWS Config also updates the Custom Conformance Pack page with a walkthrough on how to create a conformance pack YAML file from scratch. | August 25, 2022 |

| | | |
|---|---|---|
| AWS Systems Manager Document (SSM document) Integration with Conformance Packs | With this release, you can create a conformance pack template with an SSM document. For more informati on on SSM documents, see AWS Systems Manager Documents in the AWS Systems Manager User Guide.<br><br>The following data types are updated:<br><br>• PutConformancePack<br>• ConformancePackDetail<br>• TemplateSSMDocumen tDetails<br><br>The following pages in the developer guide are updated:<br><br>• Deploying a Conformance Pack Using the AWS Config Console<br>• Deploying a Conforman ce Pack Using the AWS Command Line Interface | August 24, 2022 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Simple Email Service (Amazon SES), AWS DataSync, and AWS Cloud Map. For more information, see AWS managed policies for AWS Config. | August 22, 2022 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Athena, Amazon Detective, Amazon SageMaker AI, Amazon Route 53, AWS Database Migration Service (AWS DMS), AWS Glue, AWS Key Management Service (AWS KMS), and Amazon Simple Email Service (Amazon SES) resource types. For more information, see Supported Resource Types. | August 16, 2022 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance packs:<br>• Operational Best Practices for NIST 1800 25<br>• Operational Best Practices for NIST 800 181<br>• Operational Best Practices for ABS CCIG 2.0 Standard Workloads<br>• Operational Best Practices for ABS CCIG 2.0 Material Workloads<br>• Operational Best Practices for ACSC Essential 8<br>• Operational Best Practices for ACSC ISM<br>• Operational Best Practices for APRA CPG 234<br>• Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1<br>• Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2<br>• Operational Best Practices for BNM RMiT<br>• Operational Best Practices for NIST CSF | August 1, 2022 |

| | | |
|---|---|---|
| Compliance score for conformance packs | With this release, AWS Config introduces compliance score for conformance packs, which provides you with a high-level view of the compliance state of your conformance packs. You can use it to identify, investigate, and understand the level of compliance in your conformance packs. A compliance score is the percentage of the number of compliant rule-resource combinations in a conformance pack compared to the number of total possible rule-resource combinations in the conformance pack.<br><br>The following data types are updated:<br><br>• ListConformancePackComplianceScores<br>• ConformancePackComplianceScore<br><br>The following pages in the developer guide are updated:<br><br>• Viewing the AWS Config Dashboard<br>• Viewing Compliance Data in the Conformance Packs Dashboard | July 26, 2022 |

| | | |
|---|---|---|
| | • Managing Conformance Packs (API) | |
| Security IAM update | The `ConfigConformsServiceRolePolicy` policy now grants permission to publish metric data points to Amazon CloudWatch. For more information, see AWS managed policies for AWS Config. | July 25, 2022 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon Quick Suite, Amazon Rekognition, AWS RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES), AWS Amplify, AWS AppConfig, AWS AppSync, AWS Billing Conductor, AWS DataSync, AWS Firewall Manager, AWS Glue, AWS IAM Identity Center (IAM Identity Center), EC2 Image Builder, and Elastic Load Balancing. For more information, see AWS managed policies for AWS Config. | July 15, 2022 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Compute Cloud (Amazon EC2) resource types. For more informati on, see Supported Resource Types. | July 8, 2022 |
| AWS Config supports new resources type | With this release, you can use AWS Config to record configuration changes to new AWS Global Accelerat or resource types. For more information, see Supported Resource Types. | July 5, 2022 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• autoscaling-launch-template<br>• ecs-task-definition-log-con figuration<br>• ecs-awsvpc-networking-enabled | July 1, 2022 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br><br>• Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile<br>• Operational Best Practices for Gramm Leach Bliley Act (GLBA)<br>• Operational Best Practices for GxP EU Annex 11<br>• Security Best Practices for Amazon Elastic Kubernetes Service (Amazon EKS)<br>• Security Best Practices for Amazon Relational Database Service (Amazon RDS)<br>• Security Best Practices for AWS Lambda<br><br>The following conformance packs are updated:<br><br>• Operational Best Practices for AI and ML<br>• Operational Best Practices for Amazon DynamoDB<br>• Operational Best Practices for CIS Critical Security Controls v8 IG1 | June 30, 2022 |

| | | |
|---|---|---|
| | • Operational Best Practices for CIS Critical Security Controls v8 IG2<br>• Operational Best Practices for CIS Critical Security Controls v8 IG3<br>• Operational Best Practices for HIPAA Security<br>• Operational Best Practices for NIST 800-53 rev 5<br>• Operational Best Practices for NIST CSF | |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon SageMaker AI resource types. For more information, see Supported Resource Types. | June 29, 2022 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Route 53, Amazon WorkSpaces, AWS Batch, AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), AWS Database Migration Service (AWS DMS), AWS Step Functions, and Elastic Load Balancing resource types. For more information, see Supported Resource Types. | June 14, 2022 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• aurora-last-backup-recovery-point-created<br>• dynamodb-last-backup-recovery-point-created<br>• ebs-last-backup-recovery-point-created<br>• ec2-last-backup-recovery-point-created<br>• efs-last-backup-recovery-point-created<br>• fsx-last-backup-recovery-point-created<br>• rds-last-backup-recovery-point-created<br>• s3-last-backup-recovery-point-created<br>• storagegateway-last-backup-recovery-point-created<br>• virtualmachine-last-backup-recovery-point-created | June 13, 2022 |

| | | |
|---|---|---|
| AWS Config Integration with AWS Security Hub CSPM | With this release, you can see the results of AWS Config managed and custom rule evaluations as findings in AWS Security Hub CSPM. Security Hub CSPM transforms rule evaluations into findings, which provide more information about the impacted resources, such as the Amazon Resource Name (ARN) and creation date. These findings can be viewed alongside other Security Hub CSPM findings, providing a comprehensive overview of your security posture. For more information, see Sending Rule Evaluations to Security Hub CSPM | June 7, 2022 |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for Amazon Athena, Amazon Detective, Amazon GuardDuty, Amazon Macie, Amazon Simple Email Service (Amazon SES), AWS Glue, AWS Resource Access Manager (AWS RAM), and AWS IAM Identity Center. For more information, see AWS managed policies for AWS Config. | May 31, 2022 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Security Best Practices for Amazon Elastic Container Service (Amazon ECS)<br>• Security Best Practices for Amazon Elastic File System (Amazon EFS)<br>• Security Best Practices for Amazon CloudFront<br>• Security Best Practices for AWS Auto Scaling<br>• Security Best Practices for AWS Network Firewall<br>• Security Best Practices for AWS Secrets Manager | May 31, 2022 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon SageMaker AI and AWS Step Functions resource types. For more informati on, see Supported Resource Types. | May 26, 2022 |
| AWS Config supports new conformance pack | With this release, AWS Config updates the Operational Best Practices for NERC CIP BCSI conformance pack. | May 20, 2022 |

| | | |
|---|---|---|
| Components of an AWS Config Rule | With this release, AWS Config introduces a Components of an AWS Config Rule page. The page discusses the structure of rule definitions, rule metadata, and best practices on how to write rules with Python using the AWS Config Rules Development Kit (RDK) and AWS Config Rules Development Kit Library (RDKlib). | May 9, 2022 |
| Service limits increase for organization conformance packs | With this release, AWS Config supports 180 AWS Config rules per account across all organization conformance packs. For more information, see Service Limits. | May 6, 2022 |
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Security Best Practices for Amazon OpenSearch Service<br>• Security Best Practices for Amazon Redshift<br>• Security Best Practices for AWS CloudTrail<br>• Security Best Practices for AWS CodeBuild<br>• Security Best Practices for AWS WAF | April 29, 2022 |

| | | |
|---|---|---|
| AWS Config updates managed rule | With this release, AWS Config supports the s3-resources-protected-by-backup-plan managed rule. | April 11, 2022 |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions to get information about all or a specified AWS CloudTrail event data store (EDS), get information about all or a specified AWS CloudFormation resource, get a list of a DynamoDB Accelerator (DAX) parameter group or subnet group, get information about AWS Database Migration Service (AWS DMS) replication tasks for your account in the current region being accessed, and get a list all policies in an AWS Organizations of a specified type. For more information, see AWS managed policies for AWS Config. | April 7, 2022 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• alb-desync-mode-check<br>• autoscaling-capacity-rebalancing<br>• autoscaling-launchconfig-requires-imdsv2<br>• autoscaling-launch-config-hop-limit<br>• autoscaling-multiple-instance-types<br>• clb-desync-mode-check<br>• ecs-container-insights-enabled<br>• ecs-fargate-latest-platform-version<br>• netfw-policy-default-action-fragment-packets<br>• netfw-policy-default-action-full-packets<br>• netfw-policy-rule-group-associated<br>• redshift-audit-logging-enabled<br>• s3-lifecycle-policy-check<br>• waf-regional-rule-not-empty<br>• waf-regional-rulegroup-not-empty<br>• waf-regional-webacl-not-empty | April 4, 2022 |

- vpc-peering-dns-resolution-check

| | | |
|---|---|---|
| AWS Config Custom Policy rules | With this release, AWS Config allows you to create AWS Config Custom Policy rules using AWS CloudFormation Guard (guard). Guard is a policy-as-code language that allows you to write policies that are enforced by AWS Config without the need to create Lambda functions to manage your custom rules. Rules written using Guard policy can be created from the AWS Config console or by using the AWS Config rule APIs.<br><br>The following pages in the developer guide are updated:<br><br>• AWS Config Custom Rules<br>• Creating AWS Config Custom Rules with Guard<br><br>The following data types are updated:<br><br>• Source<br>• CustomPolicyDetails<br>• ConfigRuleEvaluationStatus<br>• GetCustomRulePolicy<br>• GetOrganizationCustomRulePolicy<br>• OrganizationCustomPolicyRuleMetadata | April 4, 2022 |

| | | |
|---|---|---|
| AWS Config supports new resources type | With this release, you can use AWS Config to record configuration changes to the new Amazon EMR SecurityConfiguration resource type. For more information, see Supported Resource Types. | March 31, 2022 |
| AWS Config updates managed rule | With this release, AWS Config supports the virtualmachine-resources-protected-by-backup-plan managed rule. | March 29, 2022 |

| | | |
|---|---|---|
| AWS Config Integration with Amazon CloudWatch Metrics | With this release, AWS Config now supports tracking of your AWS Config usage and success metrics with Amazon CloudWatch in the AWS Config Dashboard page. CloudWatch metrics is a monitoring service which provides data about the performance of your systems, including the ability to search, graph, and build alarms on metrics about AWS resources . From the AWS Config Dashboard, you can see what traffic is driving your AWS Config usage and key metrics for failures that have occured in your workflow.<br><br>The following page is updated:<br><br>• Viewing the AWS Config Dashboard | March 29, 2022 |
| AWS Config supports new resources type | With this release, you can use AWS Config to record configuration changes to new Amazon GuardDuty Detector resource type. For more information, see Supported Resource Types. | March 24, 2022 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• clb-multiple-az<br>• cloudfront-no-deprecated-ssl-protocols<br>• cloudfront-traffic-to-origin-encrypted<br>• cloudwatch-alarm-action-enabled-check<br>• ec2-no-amazon-key-pair<br>• ec2-paravirtual-instance-check<br>• ec2-token-hop-limit-check<br>• ec2-transit-gateway-auto-vpc-attach-disabled<br>• ecr-private-lifecycle-policy-configured<br>• efs-access-point-enforce-root-directory<br>• efs-access-point-enforce-user-identity<br>• elbv2-multiple-az<br>• kinesis-stream-encrypted<br>• redshift-default-db-name-check<br>• s3-event-notifications-enabled<br>• sns-topic-message-delivery-notification-enabled | March 23, 2022 |

| | | |
|---|---|---|
| | • waf-global-rulegroup-not-empty<br>• waf-global-rule-not-empty | |
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance packs:<br>• Operational Best Practices for CIS Critical Security Controls v8 IG1<br>• Operational Best Practices for CIS Critical Security Controls v8 IG2<br>• Operational Best Practices for CIS Critical Security Controls v8 IG3<br>• Operational Best Practices for AWS Well-Architected Framework Security Pillar<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) High<br>• Operational Best Practices for MAS Notice 655<br>• Operational Best Practices for NIST 1800-25 | March 16, 2022 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant additional permissions for AWS CloudFormation. For more information, see AWS managed policies for AWS Config. | March 14, 2022 |
| AWS Config updates managed rules | With this release, AWS Config updates the following managed rules:<br>• aurora-resources-protected-by-backup-plan<br>• dynamodb-resources-protected-by-backup-plan<br>• ebs-resources-protected-by-backup-plan<br>• ec2-resources-protected-by-backup-plan<br>• efs-resources-protected-by-backup-plan<br>• fsx-resources-protected-by-backup-plan<br>• rds-resources-protected-by-backup-plan | March 10, 2022 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Container Registry Public resource types. For more informati on, see Supported Resource Types. | March 4, 2022 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Compute Cloud resource types. For more information, see Supported Resource Types. | February 28, 2022 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• codedeploy-auto-rollback-monitor-enabled<br>• codedeploy-ec2-minimum-healthy-hosts-configured<br>• codedeploy-lambda-allatonce-traffic-shift-disabled | February 25, 2022 |

| | | |
|---|---|---|
| Logging and Monitoring in AWS Config Update | With this release, AWS Config updates the Monitoring AWS Config with Amazon EventBridge Events page to replace references to Amazon CloudWatch Events. Amazon EventBridge is the preferred way to manage your events. CloudWatch Events and EventBridge are the same underlying service and API, but EventBridge provides more features. Changes you make in either CloudWatch or EventBridge will appear in each console. For more informance, see Amazon EventBridge. | February 24, 2022 |
| AWS SDK Page for AWS Config | With this release, AWS Config introduces a Using AWS Config with an AWS SDK page. AWS software development kits (SDKs) are available for many popular programming languages . Each SDK provides an API, code examples, and documentation that make it easier for developers to build applications in their preferred language. | February 24, 2022 |

| | | |
|---|---|---|
| Security IAM Role Trust policy update | With this release, AWS Config updates the IAM trust policy statement to include security protections in the trust policy that restrict access with `sourceARN` and/or `sourceAccountId` for the AWS Security Token Service (AWS STS) operation. This helps make sure that the IAM role trust policy is accessing your resources on behalf of expected users and scenarios only.<br><br>The following page is updated:<br><br>• Adding an IAM Trust Policy to your Role | February 18, 2022 |

| | | |
|---|---|---|
| Changes to Global Resource Type Recording | AWS Config now changes how new global resource types are recorded in AWS Config Recording. Global resource types are AWS resources that do not require you to specify a region at creation. Before this change, you could enable the recording of global resource types in all supported regions in AWS Config. After this change, new global resource types onboarded to AWS Config recording can only be recorded in the service's home region for the commercial partition, and AWS GovCloud (US-West) for the AWS GovCloud (US) partition. You will now be able to view the configuration items for these new global resource types only in their home region and AWS GovCloud (US-West) . For a list of home regions for global resource types onboarded after February 2022, see the table on the Recording All Supported Resource Types page. | February 18, 2022 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to get details about Elastic Beanstalk environments and a description of the settings for the specified Elastic Beanstalk configuration set, get a map of OpenSearch or Elasticsearch versions, describe the available Amazon RDS option groups for a database, and get information about a CodeDeploy deployment configuration. This policy also now grants permission to retrieve the specified alternate contact attached to an AWS account, retrieve information about an AWS Organizations policy, retrieve an Amazon ECR repository policy, retrieve information about an archived AWS Config rule, retrieve a list of Amazon ECS task definition families, list the root or parent organizational units (OUs) of the specified child OU or account, and list the policies that are attached to the specified target root, organizational unit, or account. For more informati | February 10, 2022 |

on, see AWS managed policies for AWS Config.

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• autoscaling-multiple-az<br>• codebuild-project-artifact-encryption<br>• codebuild-project-environment-privileged-check<br>• codebuild-project-logging-enabled<br>• codebuild-project-s3-logs-encrypted<br>• ec2-security-group-attached-to-eni-periodic<br>• ecr-private-image-scanning-enabled<br>• ecr-private-tag-immutability-enabled<br>• ecs-containers-nonprivileged<br>• ecs-containers-readonly-access<br>• ecs-no-environment-secrets<br>• ecs-task-definition-memory-hard-limit<br>• ecs-task-definition-nonroot-user<br>• ecs-task-definition-pid-mode-check<br>• eks-cluster-oldest-supported-version | February 10, 2022 |

| | | |
|---|---|---|
| | • eks-cluster-supported-version<br>• lambda-vpc-multi-az-check<br>• nacl-no-unrestricted-ssh-rdp<br>• netfw-stateless-rule-group-not-empty<br>• rds-cluster-default-admin-check<br>• rds-db-security-group-not-allowed<br>• rds-instance-default-admin-check<br>• redshift-default-admin-check<br>• s3-bucket-acl-prohibited<br>• s3-version-lifecycle-policy-check<br>• waf-global-webacl-not-empty | |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to create Amazon CloudWatch log groups and streams and to write logs to created log streams. For more information, see AWS managed policies for AWS Config. | February 2, 2022 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• opensearch-access-control-enabled<br>• opensearch-audit-logging-enabled<br>• opensearch-data-node-fault-tolerance<br>• opensearch-encrypted-at-rest<br>• opensearch-https-required<br>• opensearch-in-vpc-only<br>• opensearch-logs-to-cloudwatch<br>• opensearch-node-to-node-encryption-check | January 31, 2022 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to AWS CodeDeploy resource types. For more information, see Supported Resource Types. | January 5, 2022 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon SageMaker AI resource types. For more information, see Supported Resource Types. | December 20, 2021 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for ENISA Cybersecurity guide for SMEs | December 20, 2021 |
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for NIST 800 172<br>• Operational Best Practices for NIST 800 181<br><br>The following conformance pack is updated:<br>• Operational Best Practices for K-ISMS | November 18, 2021 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for Amazon API Gateway<br>• Operational Best Practices for AWS Backup<br>• Operational Best Practices for CISA Cyber Essentials<br>• Operational Best Practices for DevOps<br>• Operational Best Practices for NIST Privacy Framework v1.0<br><br>The following conformance packs are updated:<br>• Operational Best Practices for FedRAMP(Low)<br>• Operational Best Practices for FedRAMP(Moderate) | October 29, 2021 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon OpenSearch Service resource types. For more information, see Supported Resource Types. | October 12, 2021 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance pack:<br>• Operational Best Practices for MAS TRMG | October 12, 2021 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance packs:<br>• Operational Best Practices for ABS CCIG 2.0 Material Workloads<br>• Operational Best Practices for ABS CCIG 2.0 Standard Workloads<br>• Operational Best Practices for ACSC Essential 8<br>• Operational Best Practices for ACSC ISM<br>• Operational Best Practices for BNM RMiT<br>• Operational Best Practices for CMMC Level 1<br>• Operational Best Practices for CMMC Level 2<br>• Operational Best Practices for CMMC Level 3<br>• Operational Best Practices for CMMC Level 4<br>• Operational Best Practices for CMMC Level 5<br>• Operational Best Practices for FDA Title 21 CFR Part 11<br>• Operational Best Practices for FFIEC<br>• Operational Best Practices for MAS Notice 655<br>• Operational Best Practices for NBC TRMG | September 30, 2021 |

| | | |
|---|---|---|
| | • Operational Best Practices for NERC CIP<br>• Operational Best Practices for NIST 800-53 rev 5 | |
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to get details about an Amazon OpenSearch Service (OpenSearch Service) domain/domains and to get a detailed parameter list for a particular Amazon Relational Database Service (Amazon RDS) DB parameter group. This policy also grants permission to get details about Amazon ElastiCache snapshots. For more information, see AWS managed policies for AWS Config. | September 8, 2021 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to new Amazon Elastic Compute Cloud resource types. For more information, see Supported Resource Types. | September 7, 2021 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config updates the following conformance packs:<br>• Operational Best Practices for APRA CPG 234<br>• Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1<br>• Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2<br>• Operational Best Practices for NCSC Cloud Security Principles<br>• Operational Best Practices for NCSC Cyber Assesment Framework<br>• Operational Best Practices for NIST 800 171<br>• Operational Best Practices for NIST CSF<br>• Operational Best Practices for RBI Cyber Security Framework for UCBs<br>• Operational Best Practices for RBI MD-ITF<br>• Operational Best Practices for NYDFS 23<br>• Operational Best Practices for PCI DSS 3.2.1 | August 30, 2021 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• aurora-resources-protected-by-backup-plan<br>• backup-plan-min-frequency-and-min-retention-check<br>• backup-recovery-point-encrypted<br>• backup-recovery-point-manual-deletion-disabled<br>• backup-recovery-point-minimum-retention-check<br>• dynamodb-resources-protected-by-backup-plan<br>• ebs-resources-protected-by-backup-plan<br>• ec2-resources-protected-by-backup-plan<br>• efs-resources-protected-by-backup-plan<br>• fsx-resources-protected-by-backup-plan<br>• rds-resources-protected-by-backup-plan | August 20, 2021 |
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance pack:<br>• Operational Best Practices for NZISM | August 20, 2021 |

| | | |
|---|---|---|
| Security Amazon SNS policy update | With this release, AWS Config updates the IAM policy statement for the Amazon SNS topic when using service-linked roles to include security protectio ns that restrict access with `sourceARN` and/or `sourceAccountId` in the topic policy. This helps make sure Amazon SNS is accessing your resources on behalf of expected users and scenarios only.<br><br>The following page is updated:<br><br>• Permissions for the Amazon SNS Topic | August 17, 2021 |

| | | |
|---|---|---|
| Security AWS Lambda policy update | With this release, AWS Config updates the AWS Lambda resource-based policy for AWS Config custom rules to include security protections that restrict access with `sourceARN` and/or `sourceAccountId` in the invoke request. This helps make sure AWS Lambda is accessing your resources on behalf of expected users and scenarios only.<br><br>The following pages are updated:<br><br>• AWS::Config::ConfigRule<br>• Developing a Custom Rule for AWS Config | August 12, 2021 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to Amazon Kinesis resource types. For more informati on, see Supported Resource Types. | August 6, 2021 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance pack:<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) High<br><br>The following conformance packs are updated:<br>• Operational Best Practices for AWS Well-Architected Framework Reliability Pillar<br>• Operational Best Practices for AWS Well-Architected Framework Security Pillar<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium<br>• Operational Best Practices for HIPAA Security | July 30, 2021 |
| Example AWS Lambda Functions for AWS Config Custom Rules | With this release, AWS Config provides Python example functions in Example AWS Lambda Functions for AWS Config Rules (Python). | July 29, 2021 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to list tags for a log group, list tags for a state machine, and list all state machines. These policies now grant permission to get details about a state machine. These policies also now support additional permission for Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service, AWS Database Migration Service, AWS Global Accelerator, and AWS Storage Gateway. For more information, see AWS managed policies for AWS Config. | July 28, 2021 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to AWS Backup resource types. For more information, see Supported Resource Types. | July 14, 2021 |

| | | |
|---|---|---|
| AWS Config supports new conformance packs | With this release, AWS Config supports the following conformance packs:<br>• Operational Best Practices for CIS Critical Security Controls v8 IG1<br>• Operational Best Practices for CIS Critical Security Controls v8 IG2<br>• Operational Best Practices for CIS Critical Security Controls v8 IG3<br>• Operational Best Practices for NIST 1800 25 | July 9, 2021 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• ssm-document-not-public<br>• s3-account-level-public-access-blocks-periodic | June 25, 2021 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• ec2-instance-multiple-eni-check<br>• elbv2-acm-certificate-required<br>• autoscaling-launch-config-public-ip-disabled | June 10, 2021 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to view the permissions of AWS Systems Manager documents and information about IAM Access Analyzer. These policies now support additional AWS resource types for Amazon Kinesis, Amazon ElastiCache, Amazon EMR, AWS Network Firewall, Amazon Route 53, and Amazon Relational Database Service (Amazon RDS). These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types. These policies also now support filtering Lambda@Edge functions for the lambda-inside-vpc AWS Config managed rule. For more information, see AWS managed policies for AWS Config. | June 8, 2021 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• elasticsearch-logs-to-cloudwatch<br>• rds-cluster-multi-az-enabled<br>• api-gw-associated-with-waf<br>• iam-policy-no-statements-with-full-access | May 19, 2021 |
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to Amazon Elastic File System resource types. For more information, see Supported Resource Types. | May 13, 2021 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grants permission that allow AWS Config to make read-only GET calls to API Gateway to support a Config Rule for API Gateway. These policies also adds permissions that allow AWS Config to invoke Amazon Simple Storage Service (Amazon S3) read-only APIs, which are required to support the new `AWS::S3::AccessPoint` resource type. For more information, see AWS managed policies for AWS Config. | May 10, 2021 |
| AWS Config Custom Rules | The following pages in the developer guide are updated:<br>• Getting Started with Custom Rules for AWS Config<br>• Developing a Custom Rule for AWS Config | April 30, 2021 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• aurora-mysql-backtracking-enabled<br>• ec2-instance-profile-attached<br>• ecs-task-definition-user-for-host-mode-check<br>• no-unrestricted-route-to-igw<br>• rds-automatic-minor-version-upgrade-enabled<br>• redshift-enhanced-vpc-routing-enabled | April 15, 2021 |

| | | |
|---|---|---|
| Security IAM update | The `AWSConfigServiceRolePolicy` policy and `AWS_ConfigRole` policy now grant permission to view information about AWS Systems Manager specified documents. These policies also now support additional AWS resource types for AWS Backup, Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis, Amazon SageMaker AI, AWS Database Migration Service, and Amazon Route 53. These permission changes allow AWS Config to invoke the read-only APIs required to support these resource types. For more information, see AWS managed policies for AWS Config. | April 14, 2021 |

| | | |
|---|---|---|
| Conformance Pack Compliance as Configuration Items (CIs) | With this release, AWS Config supports conformance pack compliance as configuration items. This enables you to:<br>• View a timeline of changes to the compliance state of your conformance packs<br>• Aggregate conformance packs compliance across multiple accounts and regions<br>• Use advanced queries to check the compliance of your conformance packs<br><br>The following data types are updated:<br>• DescribeAggregateComplianceByConformancePacks<br>• GetAggregateConformancePackComplianceSummary<br><br>The following pages in the developer guide are updated:<br>• Viewing Compliance Data in the Conformance Packs Dashboard<br>• Viewing Compliance History Timeline for Conformance Packs | March 30, 2021 |

| | | |
|---|---|---|
| | • Viewing Compliance Data in the Aggregator Dashboard<br>• Querying the Current Configuration State of AWS Resources<br>• Supported Resource Types | |
| Pagination update | With this release, AWS Config advanced queries feature now supports paginatio n for queries that contain aggregate functions, such as COUNT and SUM. You can now use advanced queries to get complete results for your aggregate queries through pagination, which were previously limited to 500 rows. For more informati on, see Querying the Current Configuration State of AWS Resources | March 26, 2021 |
| Region support | With this release, AWS Config and AWS Config Rules is now supported in Asia Pacific (Osaka) Region. | March 4, 2021 |

| | | |
|---|---|---|
| AWS Config supports new resources types | With this release, you can use AWS Config to record configuration changes to Amazon Elastic Container Registry, Amazon Elastic Container Service, and Amazon Elastic Kubernete s Service resource types. For more information, see Supported Resource Types. | February 25, 2021 |
| KMS encryption support | With this release, AWS Config allows you to use KMS-based encryption on objects delivered by AWS Config for S3 bucket delivery.<br><br>The following data types are updated:<br><br>• DeliveryChannel<br>• PutDeliveryChannel<br><br>The following pages in the developer guide are updated:<br><br>• Permissions for the KMS Key<br>• Permissions for the IAM Role Assigned to AWS Config | February 16, 2021 |

| | | |
|---|---|---|
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• secretsmanager-secret-periodic-rotation<br>• secretsmanager-secret-unused<br>• secretsmanager-using-cmk | February 16, 2021 |
| Saved Query Region support | With this release, saved query is now supported in AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions. | February 15, 2021 |
| Multi-account multi-region data aggregation Region support | With this release, multi-account multi-region data aggregation is now supported in Africa (Cape Town) and Europe (Milan) Regions. For more information, see Multi-Account Multi-Region Data Aggregation. | February 15, 2021 |
| Advanced queries Region support | With this release, advanced queries is now supported in Africa (Cape Town) and Europe (Milan) Regions. For more information, see Querying the Current Configuration State of AWS Resources. | February 15, 2021 |
| AWS Config documentation history notification available through RSS feed | You can now receive notificat ion about updates to the AWS Config documentation by subscribing to an RSS feed. | January 1, 2021 |

# Earlier Updates

The following table describes the documentation release history of AWS Config prior to Dec 31, 2020.

| Change | Description | Release Date |
| --- | --- | --- |
| Saved Query support | With this release, AWS Config allows you to save your queries. After you save the query, you can search it, copy it to the query editor, edit it, or delete it. For more information about how to save a query, see the Query Using the SQL Query Editor for AWS Config (Console) and Query Using the SQL Query Editor for AWS Config (AWS CLI).<br><br>For more information about APIs, see the *AWS Config API Reference*:<br><br>• PutStoredQuery<br>• GetStoredQuery<br>• ListStoredQueries<br>• DeleteStoredQuery<br><br>Also see Service Limits for AWS Config. | December 21, 2020 |
| Process checks support | With this release, AWS Config supports process checks that is a type of AWS Config rule that allows you to track your external and internal tasks that require verificat ion as part of the conformance packs. With process checks, you can | December 17, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| | list the compliance of requirements and actions at a single location.<br><br>For more information about process checks, see the AWS Config Process Checks Within a Conformance Pack for AWS Config topic and the PutExternalEvaluation API. | |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br><br>• api-gw-ssl-enabled<br>• api-gw-xray-enabled<br>• beanstalk-enhanced-health-reporting-enabled<br>• cloudfront-accesslogs-enabled<br>• cloudfront-associated-with-waf<br>• cloudfront-custom-ssl-certificate<br>• elastic-beanstalk-managed-updates-enabled<br>• rds-cluster-iam-authentication-enabled<br>• redshift-cluster-kms-enabled<br>• s3-bucket-level-public-access-prohibited<br>• subnet-auto-assign-public-ip-disabled<br>• vpc-network-acl-unused-check | December 17, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports AWS Network Firewall | With this release, you can use AWS Config to record configuration changes to your AWS Network Firewall FirewallPolicy, RuleGroup , and Firewall resource types. For more information, see Supported Resource Types for AWS Config. | December 4, 2020 |
| Documentation update | AWS Config added support for organization-wide resource data aggregation in a delegated administrator account. You can now use a delegated administr ator account to aggregate resource configuration and compliance data from all member accounts of an organization in AWS Organizations.<br><br>For more information, see PutConfig urationAggregator, Creating Aggregators for AWS Config and Registering a Delegated Administr ator for AWS Config. | December 4, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new conformance packs | • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low<br>• Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium<br>• Operational Best Practices for NCSC Cyber Assesment Framework<br>• Operational Best Practices for RBI Cyber Security Framework for UCBs | October 30, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new conformance packs | • Operational Best Practices for ACSC Essential 8<br>• Operational Best Practices for ACSC ISM - Part 1<br>• Operational Best Practices for AI and ML<br>• Operational Best Practices for Asset Management<br>• Operational Best Practices for BCP and DR<br>• Operational Best Practices for EC2<br>• Operational Best Practices for K-ISMS<br>• Operational Best Practices for Load Balancing<br>• Operational Best Practices for Logging<br>• Operational Best Practices for Monitoring<br>• Operational Best Practices for Serverless | October 22, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new conformance packs | • Operational Best Practices for APRA CPG 234<br>• Operational Best Practices for FedRAMP(Low)<br>• Operational Best Practices for MAS Notice 655<br>• Operational Best Practices for NBC TRMG<br>• Operational Best Practices for NCSC Cloud Security Principles<br>• Operational Best Practices for RBI MD-ITF | October 15, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new conformance packs | • Operational Best Practices for ABS CCIG 2.0 Material Workloads<br>• Operational Best Practices for ABS CCIG 2.0 Standard Workloads<br>• Operational Best Practices for BNM RMiT<br>• Operational Best Practices for Data Resiliency<br>• Operational Best Practices for Data Lakes and Analytics Services<br>• Operational Best Practices for Encryption and Key Management<br>• Operational Best Practices for FDA Title 21 CFR Part 11<br>• Operational Best Practices for Publicly Accessible Resources<br>• Operational Best Practices for MAS TRMG<br>• Operational Best Practices for NERC CIP BCSI<br>• Operational Best Practices for NYDFS 23 | October 8, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new conformance packs | • Operational Best Practices for AWS Well-Architected Framework Reliability Pillar<br>• Operational Best Practices for AWS Well-Architected Framework Security Pillar<br>• Operational Best Practices for Compute Services<br>• Operational Best Practices for Databases Services<br>• Operational Best Practices for Management and Governance Services<br>• Operational Best Practices for Networking and Content Delivery Services<br>• Operational Best Practices for Security, Identity, and Compliance Services<br>• Operational Best Practices for Storage Services | October 26, 2020 |
| AWS Config supports new conformance packs | • Operational Best Practices for FedRAMP(Moderate)<br>• Operational Best Practices for FFIEC<br>• Operational Best Practices for HIPAA Security<br>• Operational Best Practices for NIST 800-53 rev 4<br>• Operational Best Practices for NIST 800 171 | September 28, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| Documentation update | The following conformance pack topics are updated.<br>• Prerequisite for Conformance Packs for AWS Config<br>• Deploying Conformance Packs for AWS Config<br>• Managing Conformance Packs for AWS Config Across all Accounts in Your Organization | September 28, 2020 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• iam-customer-policy-blocked-kms-actions<br>• iam-inline-policy-blocked-kms-actions | September 17, 2020 |
| AWS Config supports AWS WAFv2 | With this release, you can use AWS Config to record configura tion changes to your AWS WAFv2 WebACL, IPSet, RegexPatternSet, RuleGroup, and ManagedRuleSet resource types. For more informati on, see Supported Resource Types for AWS Config. | September 1, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| Documentation update | A note has been added to Full access to AWS Config about creating custom permissions that grant full access.<br><br>The documentation has been updated for the following rules:<br><br>• s3-bucket-server-side-encryption-enabled<br>• ec2-instance-detailed-monitoring-enabled<br>• ec2-managedinstance-platform-check | August 24, 2020 |
| Documentation update | Operational Best Practices for PCI DSS 3.2.1 and Operational Best Practices for NIST CSF templates are updated. | August 14, 2020 |
| Documentation update | Example relationship queries are added. For more information, see Example Relationship Queries for AWS Config. | July 30, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| Documentation update | The following data types are updated:<br>• ConfigurationAggregator<br>• RemediationConfiguration<br>• DescribeOrganizationConfigRules<br>• GetOrganizationConfigRuleDetailedStatus<br>• DescribeOrganizationConfigRuleStatuses<br>• DescribeOrganizationConformancePacks<br>• DescribeOrganizationConformancePackStatuses<br>• GetOrganizationConformancePackDetailedStatus | July 23, 2020 |
| AWS Config supports AWS Systems Manager resource type | With this release, you can use AWS Config to record configuration changes to the AWS Systems Manager file data resource type. For more information, see Supported Resource Types for AWS Config. | July 9, 2020 |
| Documentation update | Operational Best Practices for AWS Identity And Access Management and Operational Best Practices for PCI DSS 3.2.1 templates are updated. | July 9, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• account-part-of-organizations<br>• alb-http-drop-invalid-header-enabled<br>• alb-waf-enabled<br>• cloudfront-default-root-object-configured<br>• cloudfront-origin-access-identity-enabled<br>• cloudfront-origin-failover-enabled<br>• cloudfront-sni-enabled<br>• cloudtrail-security-trail-enabled<br>• cw-loggroup-retention-period-check<br>• dax-encryption-enabled<br>• dynamodb-in-backup-plan<br>• ebs-in-backup-plan<br>• ec2-imdsv2-check<br>• efs-in-backup-plan<br>• eks-endpoint-no-public-access<br>• eks-secrets-encrypted<br>• elasticsearch-node-to-node-encryption-check<br>• elb-cross-zone-load-balancing-enabled<br>• elb-tls-https-listeners-only<br>• iam-no-inline-policy-check | July 9, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| | • rds-cluster-deletion-protection-enabled<br>• rds-in-backup-plan<br>• rds-instance-deletion-protection-enabled<br>• rds-instance-iam-authentication-enabled<br>• rds-logging-enabled<br>• redshift-backup-enabled<br>• waf-classic-logging-enabled<br>• wafv2-logging-enabled<br><br>For more information, see List of AWS Config Managed Rules. | |
| Multi-account multi-region data aggregation Region support | With this release, multi-account multi-region data aggregation is now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain) Regions. For more information, see Multi-Account Multi-Region Data Aggregation and Troubleshooting for Multi-Account Multi-Region Data Aggregation for AWS Config. | July 1, 2020 |
| Advanced queries Region support | With this release, advanced queries is now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain) Regions. For more information, see Querying the Current Configuration State of AWS Resources with AWS Config. | July 1, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| Documentation update | The documentation has been updated for the following rules:<br>• ec2-managedinstance-association-compliance-status-check<br>• iam-policy-no-statements-with-admin-access<br>• required-tags<br>• restricted-common-ports<br>• rds-snapshots-public-prohibited<br>• s3-bucket-policy-grantee-check | June 30, 2020 |
| Documentation update | The documentation has been updated with information about security for AWS Config. See Security in AWS Config. | June 24, 2020 |
| Documentation update | AWS Control Tower Detective Guardrails Conformance Pack template is updated. For more information, see AWS Control Tower Detective Guardrails Conformance Pack. | June 4, 2020 |
| AWS Config supports a new conformance pack | With this release, AWS Config supports Operational Best Practices for NIST CSF conformance pack. For more information, see Operational Best Practices for NIST CSF . | May 29, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• dynamodb-pitr-enabled<br>• dynamodb-table-encrypted-kms<br>• ec2-ebs-encryption-by-default<br>• rds-snapshot-encrypted<br>• redshift-require-tls-ssl<br>• s3-bucket-default-lock-enabled<br>• s3-default-encryption-kms<br>• securityhub-enabled<br>• sns-encrypted-kms<br><br>For more information, see List of AWS Config Managed Rules. | May 28, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| Delegated administrator support | With this release, you can deploy AWS Config rules and conformance packs from any delegated member account in your organization, in addition to the management account.<br><br>For more information about APIs, see the *AWS Config API Reference*:<br><br>• PutOrganizationConfigRule<br>• PutOrganizationConformancePack<br>• DescribeOrganizationConfigRules<br>• GetOrganizationConfigRuleDetailedStatus<br>• DescribeOrganizationConfigRuleStatuses<br>• DeleteOrganizationConfigRule<br>• DeleteOrganizationConformancePack<br>• DescribeOrganizationConformancePacks<br>• DescribeOrganizationConformancePackStatuses<br>• GetOrganizationConformancePackDetailedStatus<br><br>For more information, see Service Limits for AWS Config. | May 27, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config rules Region support | With this release, few AWS Config rules are supported in Africa (Cape Town) and Europe (Milan) regions. For a detailed list of rules and the regions they are supported in, see List of AWS Config Managed Rules. | April 28, 2020 |
| AWS Config supports new conformance packs | With this release, AWS Config supports two conformance packs.<br>• AWS Control Tower Detective Guardrails Conformance Pack<br>• Operational Best Practices for CIS<br><br>For more information, see Conformance Pack Sample Templates for AWS Config. | April 22, 2020 |
| AWS Config supports AWS Secrets Manager | With this release, you can use AWS Config to record configuration changes to your Secrets Manager secret. For more information, see Supported Resource Types for AWS Config. | April 20, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• secretsmanager-rotation-enabled-check<br>• secretsmanager-scheduled-rotation-success-check<br><br>For more information, see List of AWS Config Managed Rules. | April 16, 2020 |
| Conformance pack Region support | With this release, conformance packs are now supported in Asia Pacific (Hong Kong) and Middle East (Bahrain). For more information, see Conformance Packs. | April 8, 2020 |
| Documentation update | AWS Config limits are available in this developer guide. For more information, see Service Limits for AWS Config. | April 8, 2020 |
| Documentation update | Third-party resources that are managed (that is, created/updated/deleted) through CloudFormation registry are automatically tracked in AWS Config as configuration items. For more information, see Recording Configurations with AWS Config for Third-Party Resources using the AWS CLI. | March 30, 2020 |

| Change | Description | Release Date |
|---|---|---|
| Documentation update | The AWS Config Managed Rules are updated to include AWS Region information. For more information, see List of AWS Config Managed Rules. | March 27, 2020 |
| AWS Config supports Amazon SNS resource type | With this release, you can use AWS Config to record configura tion changes to your Amazon SNS topic. For more information, see Supported Resource Types for AWS Config. | March 6, 2020 |
| Multi-account multi-region data aggregati on Region support | With this release, multi-account multi-region data aggregation is now supported in Europe (Stockhol m) Region. For more information, see Multi-Account Multi-Region Data Aggregation. | March 5, 2020 |
| Advanced queries Region support | With this release, advanced queries is now supported in Europe (Stockholm) Region. For more information, see Querying the Current Configuration State of AWS Resources with AWS Config. | March 5, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config allows you to run advanced queries with configuration aggregators | With this release, AWS Config adds support to run advanced queries based on resource configuration properties with configuration aggregators, enabling you to run the same queries across multiple accounts and Regions. For more information, see Querying the Current Configuration State of AWS Resources with AWS Config.<br><br>With this release, AWS Config adds `SelectAggregateResourceConfig` API. For more information, see SelectAggregateResourceConfig in the *AWS Config API Reference*: | February 28, 2020 |
| AWS Config supports Amazon SQS resource type | With this release, you can use AWS Config to record configuration changes to your Amazon SQS queue.<br><br>For more information, see Supported Resource Types for AWS Config. | February 13, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS CloudFormation support for Conformance packs | With this release, AWS CloudFormation support for the following resources was added: `AWS::Config::ConformancePack` and `OrganizationConformancePack`.<br><br>• AWS::Config::ConformancePack<br><br>Use the `AWS::Config::ConformancePack` resource to create a Conformance Pack that is a collection of AWS Config rules that can be easily deployed in an account and a Region and across AWS Organization.<br><br>• AWS::Config::OrganizationConformancePack<br><br>Use the `AWS::Config::OrganizationConformancePack` resource to create an Organization Conformance Pack that has information about conformance packs that AWS Config creates in the member accounts. | February 13, 2020 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• api-gw-execution-logging-enabled<br>• ec2-stopped-instance<br>• elasticache-redis-cluster-automatic-backup-check<br>• emr-master-no-public-ip<br>• guardduty-non-archived-findings<br>• rds-enhanced-monitoring-enabled<br>• s3-account-level-public-access-blocks<br>• sagemaker-endpoint-configuration-kms-key-configured<br>• service-vpc-endpoint-enabled<br><br>For more information, see List of AWS Config Managed Rules. | December 20, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| Record configurations for custom resource types | With this release, AWS Config introduces support to record configurations for custom resource types. You can publish the configuration data of third-party resources into AWS Config and view and monitor the resource inventory and configuration history using AWS Config console and APIs. For more information, see Recording Configurations with AWS Config for Third-Party Resources using the AWS CLI.<br><br>For more information about APIs, see the *AWS Config API Reference*:<br><br>• DeleteResourceConfig<br>• PutResourceConfig | November 20, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| Conformance packs | With this release, AWS Config introduces conformance packs. Conformance packs enable you to package a collection of AWS Config rules and remediation actions that can then be deployed together as a single entity across an entire AWS Organization. For more information, see Conformance Packs.<br><br>For more information about APIs, see the *AWS Config API Reference*:<br><br>• DeleteOrganizationConformancePack<br>• DeleteOrganizationConformancePack<br>• DescribeConformancePacks<br>• DescribeConformancePacks<br>• DescribeConformancePackStatus<br>• DescribeOrganizationConformancePacks<br>• DescribeOrganizationConformancePackStatuses<br>• GetConformancePackComplianceDetails<br>• GetConformancePackComplianceSummary<br>• GetOrganizationConformancePackDetailedStatus,<br>• PutConformancePack<br>• PutOrganizationConformancePack | November 19, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Amazon OpenSearch Service and AWS Key Management Service resource types | With this release, you can use AWS Config to record configuration changes to your Amazon OpenSearch Service domain and AWS Key Management Service key.<br><br>For more information, see Supported Resource Types for AWS Config. | November 11, 2019 |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br><br>• dms-replication-not-public<br>• emr-kerberos-enabled<br>• internet-gateway-authorized-vpc-only<br>• kms-cmk-not-scheduled-for-deletion<br>• sagemaker-notebook-no-direct-internet-access<br>• sagemaker-notebook-instance-kms-key-configured<br>• shield-drt-access<br><br>For more information, see List of AWS Config Managed Rules. | October 10, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Amazon RDS resource type | With this release, you can use AWS Config to record configuration changes to your Amazon Relationa l Database Service (Amazon RDS) DBCluster and DBClusterSnapshot.<br><br>For more information, see Supported Resource Types for AWS Config. | September 17, 2019 |
| AWS Config supports Amazon QLDB resource type | With this release, you can use AWS Config to record configura tion changes to Amazon Quantum Ledger Database (QLDB) ledger resource type.<br><br>For more information, see Supported Resource Types for AWS Config. | September 10, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config allows you to apply auto remediation on noncompliant resources as evaluated by AWS Config Rules | With this release, AWS Config introduces support to apply auto remediation using AWS Systems Manager automation documents on noncompliant resources as evaluated by AWS Config Rules. For more information, see Remediating Noncompliant Resources with AWS Config.<br><br>With this release, AWS Config adds the following new APIs. For more information, see the *AWS Config API Reference* :<br><br>• PutRemediationExceptions<br>• DescribeRemediationExceptions<br>• DeleteRemediationExceptions | September 5, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config supports the following managed rules:<br>• alb-http-to-https-redirection-check<br>• api-gw-cache-enabled-and-encrypted<br>• api-gw-endpoint-type-check<br>• cloudtrail-s3-dataevents-enabled<br>• cloudwatch-log-group-encrypted<br>• ebs-snapshot-public-restorable-check<br>• elb-deletion-protection-enabled<br>• lambda-concurrency-check<br>• lambda-dlq-check<br>• lambda-inside-vpc<br>• shield-advanced-enabled-autorenew<br>• vpc-vpn-2-tunnels-up<br><br>For more information, see List of AWS Config Managed Rules. | August 22, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config updates the following managed rules:<br>• cloudfront-viewer-policy-https<br>• ec2-instance-no-public-ip<br>• ec2-security-group-attached-to-eni<br>• efs-encrypted-check<br>• elasticsearch-encrypted-at-rest<br>• elasticsearch-in-vpc-only<br>• redshift-cluster-public-access-check<br>• vpc-sg-open-only-to-authorized-ports<br><br>For more information, see List of AWS Config Managed Rules. | July 31, 2019 |
| AWS Config supports Amazon EC2 resource types | With this release, you can use AWS Config to record configuration changes to the following Amazon EC2 resources; VPCEndpoint, VPCEndpointService, and VPCPeeringConnection.<br><br>For more information, see Supported Resource Types for AWS Config. | July 12, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config allows you to manage AWS Config rules across all AWS accounts within an organization | With this release, AWS Config introduces support for managing AWS Config rules across all AWS accounts within an organization. You can centrally create, update, and delete AWS Config rules across all accounts in your organizat ion. For more information, see Managing AWS Config Rules Across All Accounts in Your Organization.<br><br>For more information about APIs, see the *AWS Config API Reference*:<br><br>• PutOrganizationConfigRule<br>• DescribeOrganizationConfigRules<br>• GetOrganizationConfigRuleDe tailedStatus<br>• DescribeOrganizationConfigR uleStatuses<br>• DeleteOrganizationConfigRule | July 9, 2019 |
| AWS Config supports Amazon S3 and Amazon EC2 resource types | With this release, you can use AWS Config to record configura tion changes to the Amazon S3 AccountPublicAccessBlock resource and the following Amazon EC2 resources; NatGateway, EgressOnl yInternetGateway, and FlowLog.<br><br>For more information, see Supported Resource Types for AWS Config. | May 17, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config updates managed rules | With this release, AWS Config updates the following managed rules:<br>• s3-bucket-public-read-prohibited<br>• s3-bucket-public-write-prohibited<br><br>For more information, see List of AWS Config Managed Rules. | May 7, 2019 |
| AWS Config allows you to delete a remediati on action using AWS Management Console. | With this release, AWS Config introduces support to delete a remediation action using AWS Management Console. For more information, see Remediating Noncompliant Resources with AWS Config. | April 24, 2019 |
| AWS Config supports new managed rules | This release supports a new managed rule: fms-shield-resource-policy-check.<br><br>For more information, see List of AWS Config Managed Rules. | April 7, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Amazon API Gateway resource type | With this release, you can use AWS Config to record configuration changes to the following Amazon API Gateway resources; Api (WebSocket API), RestApi (REST API), Stage (WebSocket API stage), and Stage (REST API stage).<br><br>For more information, see Supported Resource Types for AWS Config. | March 20, 2019 |
| AWS Config allows you to run advanced queries | With this release, AWS Config adds support to run advanced queries based on resource configuration properties. For more information, see Querying the Current Configuration State of AWS Resources with AWS Config.<br><br>With this release, AWS Config adds `SelectResourceConfig` API. For more information, see SelectResourceConfig in the *AWS Config API Reference*: | March 19, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config allows you to assign tags your AWS Config resources | With this release, AWS Config introduces support for tag based access control for three AWS Config resources—`ConfigRule`, `ConfigurationAggregator`, and `AggregationAuthorization` . For more information, see Tagging Your AWS Config Resources.<br><br>With this release, you can add, remove or list tags from your AWS Config resources using the following data types. For more information, see the *AWS Config API Reference*:<br><br>• ListTagsForResource<br>• TagResource<br>• UntagResource | March 14, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config allows you to apply remediation on noncompliant resources as evaluated by AWS Config Rules | With this release, AWS Config introduces support to apply remediation using AWS Systems Manager automation documents on noncompliant resources as evaluated by AWS Config Rules. For more information, see Remediating Noncompliant Resources with AWS Config.<br><br>With this release, AWS Config adds the following new APIs. For more information, see the *AWS Config API Reference* :<br><br>• DeleteRemediationConfiguration<br>• DescribeRemediationConfigurations<br>• DescribeRemediationExecutionStatus<br>• PutRemediationConfigurations<br>• StartRemediationExecution | March 12, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports AWS Config Rules in China (Ningxia) Region | This release only supports 54 AWS Config Rules in the China (Ningxia) Region. For more information, see List of AWS Config Managed Rules.<br><br>However, AWS Config does not currently support the following rules in the China (Ningxia) Region:<br><br>• acm-certificate-expiration-check<br>• cmk-backing-key-rotation-enabled<br>• cloudformation-stack-drift-detection-check<br>• cloudformation-stack-notification-check<br>• cloud-trail-encryption-enabled<br>• cloud-trail-log-file-validation-enabled<br>• codebuild-project-envvar-awscred-check<br>• codebuild-project-source-repo-url-check<br>• codepipeline-deployment-count-check<br>• codepipeline-region-fanout-check<br>• dynamodb-table-encryption-enabled<br>• elb-acm-certificate-required<br>• encrypted-volumes<br>• fms-webacl-resource-policy-check | March 12, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| | • fms-webacl-rulegroup-association-check<br>• guardduty-enabled-centralized<br>• lambda-function-public-access-prohibited<br>• lambda-function-settings-check<br>• rds-storage-encrypted<br>• root-account-mfa-hardware-mfa-enabled<br>• root-account-mfa-enabled<br>• s3-bucket-blacklisted-actions-prohibited<br>• s3-bucket-policy-grantee-check<br>• s3-bucket-policy-not-more-permissive<br>• s3-bucket-public-read-prohibited<br>• s3-bucket-public-write-prohibited<br>• s3-bucket-server-side-encryption-enabled<br>• s3-bucket-ssl-requests-only | |
| AWS Config supports new managed rules | This release supports the following new managed rules:<br>• iam-user-mfa-enabled<br>• s3-bucket-policy-grantee-check<br><br>For more information, see List of AWS Config Managed Rules. | January 21, 2019 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Service Catalog resource type | With this release, you can use AWS Config to record configuration changes to the following Service Catalog resources; CloudFromation product, provisioned product, and portfolio. For more information, see Supported Resource Types for AWS Config. | January 11, 2019 |
| Service-linked AWS Config rules support | With this release, AWS Config adds a new managed config rule that supports other AWS services to create AWS Config Rules in your account. For more information, see Service-Linked AWS Config Rules. | November 20, 2018 |
| AWS Config allows you to aggregate configuration data of AWS resources | With this release, AWS Config introduces support for aggregati ng the configuration data of AWS resources. For more information, see Viewing Compliance and Inventory Data in the Aggregator Dashboard for AWS Config.<br><br>With this release, AWS Config adds the following new APIs. For more information, see the *AWS Config API Reference* :<br><br>• BatchGetAggregateResourceConfig<br>• GetAggregateDiscoveredResourceCounts<br>• GetAggregateResourceConfig<br>• ListAggregateDiscoveredResources | November 19, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new managed rules | This release supports the following new managed rules:<br>• cloudformation-stack-drift-detection-check<br>• codepipeline-deployment-count-check<br>• codepipeline-region-fanout-check<br><br>For more information, see List of AWS Config Managed Rules. | November 19, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new managed rules | This release supports the following new managed rules:<br>• access-keys-rotated<br>• cloud-trail-cloud-watch-logs-enabled<br>• cloud-trail-encryption-enabled<br>• cloud-trail-log-file-validation-enabled<br>• cmk-backing-key-rotation-enabled<br>• iam-policy-no-statements-with-admin-access<br>• iam-role-managed-policy-check<br>• iam-root-access-key-check<br>• iam-user-unused-credentials-check<br>• mfa-enabled-for-iam-console-access<br>• multi-region-cloudtrail-enabled<br>• root-account-hardware-mfa-enabled<br>• vpc-flow-logs-enabled<br><br>For more information, see List of AWS Config Managed Rules. | November 12, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new managed rules | This release supports the following new managed rules:<br>• dynamodb-table-encryption-enabled<br>• elb-logging-enabled<br>• rds-instance-public-access-check<br>• vpc-default-security-group-closed<br><br>For more information, see List of AWS Config Managed Rules. | October 24, 2018 |
| Compliance history support | With this release, AWS Config now supports storing compliance history of resources as evaluated by AWS Config Rules. For more information, see Viewing Compliance History Timeline for Resources and Rules. | October 18, 2018 |
| Multi-account multi-region Data Aggregation Region support | With this release, multi-account multi-region Data Aggregation is now supported in six new Regions. For more information, see Multi-Account Multi-Region Data Aggregation. | October 4, 2018 |
| AWS Config supports resource-level permissions for AWS Config Rules APIs actions | With this release, AWS Config supports resource-level permissions for certain AWS Config Rules API actions. For more information about the supported APIs, see Supported Resource-Level Permissions for AWS Config Rule API Actions. | October 1, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports CodePipeline resource type | With this release, you can use AWS Config to record configuration changes to the AWS CodePipeline resource type. For more information, see Supported Resource Types for AWS Config. | September 12, 2018 |
| AWS Config supports new managed rules | This release supports the following new managed rules:<br>• ec2-instance-managed-by-systems-manager<br>• ec2-managedinstance-association-compliance-status-check<br>• ec2-managedinstance-patch-compliance-status-check<br>• guardduty-enabled-centralized<br>• rds-snapshots-public-prohibited<br>• s3-bucket-blacklisted-actions-prohibited<br>• s3-bucket-policy-not-more-permissive<br><br>For more information, see List of AWS Config Managed Rules. | September 5, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports AWS Systems Manager resource type | With this release, you can use AWS Config to record configuration changes to the AWS Systems Manager patch compliance and association compliance resource types. For more information, see Supported Resource Types for AWS Config. | August 9, 2018 |
| AWS Config allows you to delete your AWS Config data using AWS Management Console | With this release, AWS Config introduces support for retention period using AWS Management Console. In the AWS Management Console, you can select a custom data retention period for your `ConfigurationItems`. For more information, see Deleting AWS Config Data. | August 7, 2018 |
| AWS Config supports AWS Shield resource type | With this release, you can use AWS Config to record configuration changes to the AWS Shield Protection resource type. For more information, see Supported Resource Types for AWS Config. | August 7, 2018 |
| AWS Config supports AWS PrivateLink | With this release, AWS Config supports AWS PrivateLink, enabling you to route data between your Amazon Virtual Private Cloud (VPC) and AWS Config entirely within the AWS network. For more information, see Using AWS Config with Interface Amazon VPC Endpoints. | July 31, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config allows you to delete your AWS Config data | With this release, AWS Config introduces support for retention period. AWS Config allows you to delete your data by specifying a retention period for your `ConfigurationItems`. For more information, see Deleting AWS Config Data.<br><br>With this release, AWS Config adds the following new APIs. For more information, see the *AWS Config API Reference* :<br><br>• PutRetentionConfiguration<br>• DescribeRetentionConfigurations<br>• DeleteRetentionConfiguration | May 25, 2018 |
| AWS Config supports new managed rules | This release supports the following two new managed rules:<br><br>• lambda-function-settings-check<br>• s3-bucket-replication-enabled<br>• iam-policy-blacklisted-check<br><br>For more information, see List of AWS Config Managed Rules. | May 10, 2018 |
| AWS Config supports AWS X-Ray resource type | With this release, you can use AWS Config to record configuration changes to the AWS X-Ray EncryptionConfig resource type. For more information, see Supported Resource Types for AWS Config. | May 1, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports AWS Lambda resource type and one new managed rule | With this release, you can use AWS Config to record configuration changes to the AWS Lambda function resource type. For more information, see Supported Resource Types for AWS Config.<br><br>This release also supports the lambda-function-public-access-prohibited managed rule. For more information, see AWS Config Managed Rules. | April 25, 2018 |
| AWS Config supports AWS Elastic Beanstalk resource type | With this release, you can use AWS Config to record configuration changes to the AWS Elastic Beanstalk Application, Application Version, and Environment resources.<br><br>For more information, see Supported Resource Types for AWS Config. | April 24, 2018 |
| AWS Config supports new managed rules | This release supports the following two new managed rules:<br><br>• fms-webacl-resource-policy-check<br>• fms-webacl-rulegroup-association-check<br><br>For more information, see List of AWS Config Managed Rules. | April 4, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| Multi-account multi-region data aggregation | With this release, AWS Config introduces multi-account multi-region data aggregation. This feature allows you to aggregate AWS Config data from multiple accounts or an organization and multiple regions into an aggregator account. For more information, see Multi-Account Multi-Region Data Aggregation.<br><br>With this release, AWS Config adds the following new APIs. For more information, see the *AWS Config API Reference* :<br><br>• PutConfigurationAggregator<br>• DescribePendingAggregationRequests<br>• DeletePendingAggregationRequest<br>• PutAggregationAuthorization<br>• DescribeAggregationAuthorizations<br>• GetAggregateConfigRuleComplianceSummary<br>• DescribeAggregateComplianceByConfigRules<br>• GetAggregateComplianceDetailsByConfigRule<br>• DescribeConfigurationAggregators<br>• DescribeConfigurationAggregatorSourcesStatus<br>• DeleteAggregationAuthorization | April 4, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| | • DeleteConfigurationAggregator | |
| Monitoring AWS Config with Amazon CloudWatch Events | With this release, use Amazon CloudWatch Events to detect and react to changes in the status of AWS Config events.<br><br>For more information, see Monitoring AWS Config with Amazon EventBridge. | March 29, 2018 |
| New API operation | With this release, AWS Config adds support for BatchGetResourceConfig API, allowing you to batch-retrieve the current state of one or more of your resources. | March 20, 2018 |
| AWS Config supports AWS WAF RuleGroup resource type | With this release, you can use AWS Config to record configuration changes to the AWS WAF RuleGroup and AWS WAF RuleGroup Regional resources.<br><br>For more information, see Supported Resource Types for AWS Config. | February 15, 2018 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new managed rules | This release supports the following new managed rules:<br>• elb-acm-certificate-required<br>• elb-custom-security-policy-ssl-check<br>• elb-predefined-security-policy-ssl-check<br>• codebuild-project-envvar-awscred-check<br>• codebuild-project-source-repo-url-check<br>• iam-group-has-users-check<br>• s3-bucket-server-side-encryption-enabled<br><br>For more information, see List of AWS Config Managed Rules. | January 25, 2018 |
| AWS Config supports ELB resource type | With this release, you can use AWS Config to record configuration changes to your Elastic Load Balancing classic load balancers.<br><br>For more information, see Supported Resource Types for AWS Config. | November 17, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports the Amazon CloudFront and AWS WAF resource type | With this release, you can use AWS Config to record configuration changes to your CloudFront distribut ion and streaming distribution.<br><br>With this release, you can use AWS Config to record configuration changes to the following AWS WAF and AWS WAF Regional resources; rate based rule, rule, and Web ACL.<br><br>For more information, see Supported Resource Types for AWS Config. | November 15, 2017 |
| AWS Config supports the AWS CodeBuild resource type | With this release, you can use AWS Config to record configuration changes to your AWS CodeBuild projects.<br><br>For more information, see Supported Resource Types for AWS Config. | October 20, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Auto Scaling resources and one new managed rule | With this release, you can use AWS Config to record configuration changes to the following Auto Scaling resources; groups, launch configuration, scheduled action, and scaling policy.<br><br>For more information, see Supported Resource Types for AWS Config.<br><br>This release also supports the following managed rule:<br><br>• autoscaling-group-elb-healthcheck-required<br><br>For more information, see AWS Config Managed Rules. | September 18, 2017 |
| AWS Config supports the AWS CodeBuild resource type | With this release, you can use AWS Config to record configuration changes to your AWS CodeBuild projects.<br><br>For more information, see Supported Resource Types for AWS Config. | October 20, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Auto Scaling resources and one new managed rule | With this release, you can use AWS Config to record configuration changes to the following Auto Scaling resources; groups, launch configuration, scheduled action, and scaling policy.<br><br>For more information, see Supported Resource Types for AWS Config.<br><br>This release also supports the following managed rule:<br><br>• autoscaling-group-elb-healthcheck-required<br><br>For more information, see AWS Config Managed Rules. | September 18, 2017 |
| AWS Config supports the DynamoDB table resource type and one new managed rule | With this release, you can use AWS Config to record configuration changes to your DynamoDB tables.<br><br>For more information, see Supported Resource Types for AWS Config.<br><br>This release supports the following managed rule:<br><br>• dynamodb-autoscaling-enabled<br><br>For more information, see AWS Config Managed Rules. | September 8, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports two new managed rules for Amazon S3 | This release supports two new managed rules:<br>• s3-bucket-public-read-prohibited<br>• s3-bucket-public-write-prohibited<br><br>For more information, see AWS Config Managed Rules. | August 14, 2017 |
| New page in the AWS Config console | You can use the **Dashboard** in the AWS Config console to see the following:<br>• Total number of resources<br>• Total number of rules<br>• Number of noncompliant resources<br>• Number of noncompliant rules<br><br>For more information, see Viewing the AWS Config Dashboard. | July 17, 2017 |
| New API operation | You can use the GetDiscoveredResourceCounts operation to return the number of resource types, the number of each resource type, and the total number of resources that AWS Config is recording in a Region for your AWS account. | July 17, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports the CloudFormation stack resource type and one new managed rule | With this release, you can use AWS Config to record configuration changes to your CloudFormation stacks.<br><br>For more information, see Supported Resource Types for AWS Config.<br><br>This release supports the following managed rule:<br><br>• cloudformation-stack-notification-check<br><br>For more information, see AWS Config Managed Rules. | July 6, 2017 |
| New and updated content | This release adds support for AWS Config Rules in the Canada (Central) Region and South America (São Paulo) Region.<br><br>For all regions that support AWS Config and Config Rules, see AWS Regions and Endpoints in the *AWS General Reference*. | July 5, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| New and updated content | AWS Config Rules is available in the AWS GovCloud (US) Region. For more information, see the AWS GovCloud (US) User Guide.<br><br>For regions that support AWS Config, see AWS Regions and Endpoints in the *AWS General Reference*. | June 8, 2017 |
| AWS Config supports the Amazon CloudWatch alarm resource type and three new managed rules | With this release, you can use AWS Config to record configuration changes to your Amazon CloudWatch alarms.<br><br>For more information, see Supported Resource Types for AWS Config.<br><br>This release supports three new managed rules:<br><br>• cloudwatch-alarm-action-check<br>• cloudwatch-alarm-resource-check<br>• cloudwatch-alarm-settings-check<br><br>For more information, see AWS Config Managed Rules. | June 1, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| New and updated content | This release supports specifying the application version number for the following managed rules:<br>• ec2-managedinstance-applications-blacklisted<br>• ec2-managedinstance-applications-required<br><br>For more information, see AWS Config Managed Rules. | June 1, 2017 |
| New and updated content | This release adds support for AWS Config Rules in the Asia Pacific (Mumbai) Region. For more information, see AWS Regions and Endpoints in the *AWS General Reference*. | April 27, 2017 |
| New and updated content | This release supports an updated console experience for adding AWS Config managed rules to your account for the first time.<br><br>When you set up AWS Config Rules for the first time or in a new Region, you can search for AWS managed rules by name, description, or label. You can choose **Select all** to select all rules or choose **Clear all** to clear all rules.<br><br>For more information, see Add, View, Update and Delete Rules (Console). | April 5, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports new managed rules | This release supports the following new managed rules:<br>• acm-certificate-expiration-check<br>• ec2-instance-detailed-monitoring-enabled<br>• ec2-managedinstance-inventory-blacklisted<br>• ec2-volume-inuse-check<br>• iam-user-group-membership-check<br>• iam-user-no-policies-check<br>• s3-bucket-ssl-requests-only<br><br>For more information, see List of AWS Config Managed Rules. | February 21, 2017 |
| New and updated content | This release adds support for AWS Config Rules in the Europe (London) Region. For more information, see AWS Regions and Endpoints in the *AWS General Reference*. | February 21, 2017 |
| New and updated content | This release adds CloudFormation templates for AWS Config managed rules. You can use the templates to create managed rules for your account. For more information, see Creating AWS Config Managed Rules With AWS CloudFormation Templates. | February 16, 2017 |

| Change | Description | Release Date |
| --- | --- | --- |
| New and updated content | This release adds support for a new test mode for the `PutEvaluations` API. Set the `TestMode` parameter to true in your custom rule to verify whether your AWS Lambda function will deliver evaluation results to AWS Config. No updates occur to your existing evaluations, and evaluation results are not sent to AWS Config.<br><br>For more information, see PutEvaluations in the *AWS Config API Reference*. | February 16, 2017 |
| New and updated content | This release adds support for AWS Config Rules in the Asia Pacific (Seoul), and US West (N. California) Regions. For more information, see AWS Regions and Endpoints in the *AWS General Reference*. | December 21, 2016 |
| New and updated content | This release adds support for AWS Config in the Europe (London) Region. For more information, see AWS Regions and Endpoints in the *AWS General Reference*. | December 13, 2016 |
| New and updated content | This release adds support for AWS Config in the Canada (Central) Region. For more information, see AWS Regions and Endpoints in the *AWS General Reference*. | December 8, 2016 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Amazon Redshift resource types and two new managed rules | With this release, you can use AWS Config to record configuration changes to your Amazon Redshift clusters, cluster parameter groups, cluster security groups, cluster snapshots, cluster subnet groups, and event subscriptions.<br><br>For more information, see Supported Resource Types for AWS Config.<br><br>This release supports two new managed rules:<br><br>• redshift-cluster-configuration-check<br>• redshift-cluster-maintenancesettings-check<br><br>For more information, see List of AWS Config Managed Rules. | December 7, 2016 |
| New and updated content | This release adds support for a new managed rule:<br><br>• dynamodb-throughput-limit-check<br><br>For more information, see List of AWS Config Managed Rules. | December 7, 2016 |

| Change | Description | Release Date |
| --- | --- | --- |
| New and updated content | This release adds support for creating up to 50 rules per Region in an account. For more information, see AWS Config Limits in the *AWS General Reference*. | December 7, 2016 |
| AWS Config supports the managed instance inventory resource type for Amazon EC2 Systems Manager and three new managed rules | With this release, you can use AWS Config to record software configuration changes on your managed instances with support for managed instance inventory.<br><br>For more information, see Recording Software Configuration for Managed Instances.<br><br>This release supports three new managed rules:<br><br>• ec2-managedinstance-inventory-blacklisted<br>• ec2-managedinstance-applications-required<br>• ec2-managedinstance-platform-check<br><br>For more information, see List of AWS Config Managed Rules. | December 1, 2016 |
| New and updated content | AWS Config is available in the China (Beijing) Region. | October 24, 2016 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports the Amazon S3 bucket resource and two new managed rules | With this release, you can use AWS Config to record configura tion changes to your Amazon S3 buckets. For more information, see Supported Resource Types for AWS Config.<br><br>This release supports two new managed rules:<br><br>• s3-bucket-logging-enabled<br>• s3-bucket-versioning-enabled<br><br>For more information, see AWS Config Managed Rules. | October 18, 2016 |
| New and updated content | This release adds support for AWS Config and AWS Config Rules in the US East (Ohio) Region. For more information, see AWS Regions and Endpoints in the *AWS General Reference*. | October 17, 2016 |

| Change | Description | Release Date |
| --- | --- | --- |
| New and updated managed rules | This update adds support for eight new managed rules:<br>• approved-amis-by-id<br>• approved-amis-by-tag<br>• db-instance-backup-enabled<br>• desired-instance-type<br>• ebs-optimized-instance<br>• iam-password-policy<br>• rds-multi-az-support<br>• rds-storage-encrypted<br><br>You can specify multiple parameter values for the following rules:<br>• desired-instance-tenancy<br>• required-tags<br><br>For more information, see List of AWS Config Managed Rules. | October 4, 2016 |
| New and updated content for the AWS Config console | This update adds support for viewing AWS CloudTrail API activity in the AWS Config timeline. If CloudTrail is logging for your account, you can view create, update, and delete API events for configuration changes to your resources. For more information, see Viewing Compliance History for your AWS Resources with AWS Config. | September 06, 2016 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports ELB resource type | With this release, you can use AWS Config to record configuration changes to your ELB application load balancers. For more informati on, see Supported Resource Types for AWS Config. | August 31, 2016 |
| New and updated content | This release adds support for AWS Config Rules in the Asia Pacific (Singapore), and Asia Pacific (Sydney) Regions. For more information, see AWS Regions and Endpoints in the *AWS General Reference*. | August 18, 2016 |
| New and updated content for AWS Config Rules | This update adds support for creating a rule that can be triggered by both configuration changes and at a periodic frequency that you choose. For more information, see Components of an AWS Config Rule.<br><br>This update also adds support for manually evaluating your resources against your rule and deleting evaluation results. For more information, see Evaluating Your Resources with AWS Config Rules.<br><br>This update also adds support for evaluating additional resource types using custom rules. | July 25, 2016 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports Amazon RDS and AWS Certificate Manager (ACM) resource types | With this release, you can use AWS Config to record configuration changes to your Amazon Relational Database Service (Amazon RDS) DB instances, DB security groups, DB snapshots, DB subnet groups, and event subscriptions. You can also use AWS Config to record configuration changes to certificates provided by ACM.<br><br>For more information, see Supported Resource Types for AWS Config. | July 21, 2016 |
| Updated information about managing the configura tion recorder | This update adds steps for renaming and deleting the configuration recorder to Working with the configuration recorder. | July 07, 2016 |
| Simplified role creation and updated policies | With this update, creating an IAM role for AWS Config is simplified. This enhancement is available in regions that support Config rules. To support this enhancement, the steps in Setting Up AWS Config with the Console are updated, the example policy in Permissions for the Amazon S3 Bucket for the AWS Config Delivery Channel is updated, and the example policy in Identity-based policy examples for AWS Config is updated. | March 31, 2016 |

| Change | Description | Release Date |
| --- | --- | --- |
| Example functions and events for Config rules | This update provides updated example functions. | March 29, 2016 |
| AWS Config Rules GitHub repository | This update adds information about the AWS Config Rules GitHub repository to Evaluating Resources with AWS Config Rules. This repository provides sample functions for custom rules that are developed and contributed by AWS Config users. | March 1, 2016 |
| AWS Config Rules | This release introduces AWS Config Rules. With rules, you can use AWS Config to evaluate whether your AWS resources comply with your desired configurations. For more information, see Evaluating Resources with AWS Config Rules. | December 18, 2015 |
| AWS Config supports IAM resource types | With this release, you can use AWS Config to record configuration changes to your IAM users, groups, roles, and customer managed policies. For more information, see Supported Resource Types for AWS Config. | December 10, 2015 |

| Change | Description | Release Date |
| --- | --- | --- |
| AWS Config supports EC2 Dedicated host | With this release, you can use AWS Config to record configuration changes to your EC2 Dedicated hosts. For more information, see Supported Resource Types for AWS Config. | November 23, 2015 |
| Updated permissions information | This update adds information about the following AWS managed policies for AWS Config:<br>• `AWS_ConfigRole` – Grants AWS Config permission to get configuration details about your resources. For more information, see IAM Role Policy for Getting Configuration Details.<br>• `AWSConfigUserAccess` – Grants read-only access to an AWS Config user. For more information, see Read-only access to AWS Config. | October 19, 2015 |
| AWS Config Rules preview | This release introduces the AWS Config Rules preview. With rules, you can use AWS Config to evaluate whether your AWS resources comply with your desired configurations. For more information, see Evaluating Resources with AWS Config Rules. | October 7, 2015 |

| Change | Description | Release Date |
| --- | --- | --- |
| New and updated content | This release adds the ability to look up resources that AWS Config has discovered. For more information, see Looking Up Resources That Are Discovered by AWS Config. | August 27, 2015 |
| New and updated content | This release adds the ability to select which resource types AWS Config records. For more information, see Recording AWS Resources with AWS Config. | June 23, 2015 |
| New and updated content | This release adds support for the following regions: Asia Pacific (Tokyo), Asia Pacific (Singapore), Europe (Frankfurt), South America (São Paulo), and US West (N. California). For more information, see AWS Regions and Endpoints. | April 6, 2015 |
| New guide | This release introduces AWS Config. | November 12, 2014 |